**The Emerging Document Management Requirements for Effective Cyber Security Webinar on October 11, 2017**

## Cases

- Hefter Impact Tech. v. Sport Maska Inc., 2017 WL 3317413 (D. Mass. Aug. 3, 2017)
- Martinez v. City of Chicago, 2016 WL 3538823, at *24 (N.D. Ill. June 29, 2016)
- Moody v. CSX Transportation, Inc., No. 07-CV-6398P, 2017 WL 4173358 (W.D.N.Y. Sept. 21, 2017)
- European Court of Justice Case 131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González [2014]

## Regulations

- Federal Rules of Civil Procedure 37(e) and accompanying 2015 Advisory Committee Notes
- NY DFS Regulation 23 NYCRR 500.13
- Federal Trade Commission's Five Key Principles to Protect Personal Information
- The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

2017 WL 3317413
Only the Westlaw citation is currently available.
United States District Court,
D. Massachusetts.

HEFTER IMPACT TECHNOLOGIES, LLC, Plaintiff,
v.
SPORT MASKA, INC., d/b/
a Reebok—CCM Hockey, Defendant.

Civil Action No. 15-13290-FDS
|
Signed 08/03/2017

**Attorneys and Law Firms**

Giovanni M. Ruscitti, Mary Sue Greenleaf, Berg Hill Greenleaf & Ruscitti LLP, Boulder, CO, Giles L. Krill, Law Offices of Edward A. Gottlieb, Brighton, MA, for Plaintiff.

Shepard Davidson, Laura Lee Mittelman, Burns & Levinson LLP, Boston, MA, for Defendant.

# MEMORANDUM AND ORDER ON PLAINTIFF'S MOTION FOR SANCTIONS FOR SPOLIATION OF EVIDENCE AND DISCOVERY MISCONDUCT

F. Dennis Saylor IV, United States District Judge

***1** This is a contract dispute. In 2005, plaintiff Hefter Impact Technologies, LLC, ("HIT") entered into an agreement with defendant Sport Maska, Inc., d/b/a Reebok—CCM Hockey, for the sale and assignment of a design for an ice-hockey helmet. The agreement provided for a lump-sum payment as well as the payment of royalties on the sale of certain helmets. In substance, the complaint alleges that defendant has failed to pay HIT royalties it is owed under the agreement.

HIT has filed a motion for sanctions for spoliation of evidence. For the following reasons, the motion will be granted in part and denied in part.

## I. Background

### A. Factual Background

Unless otherwise noted, the following facts are undisputed.

#### 1. Parties

Hefter Impact Technologies, LLC is a limited liability company that designs ice-hockey helmets. (Def. Mot. Summ. J. SMF ¶ 1). Defendant Sport Maska, Inc. is a corporation doing business as Reebok—CCM Hockey ("CCM") and headquartered in Montreal, Canada. (Answer ¶ 8). CCM sells ice-hockey equipment, including helmets. (Pl. Mot. Summ. J. SMF ¶ 1).

Around 2003, HIT developed a new design for an ice-hockey helmet that the parties call the "Hefter Shell Design." (*Id.* ¶ 1). [1] Dennis Hefter, the founder of HIT, testified that he created the Hefter Shell Design to appear more narrow and angular than existing helmets in order to give it a "faster" look. (Hefter Dep. 106; Pl. Mot. Summ. J. SMF ¶ 2).

#### 2. Purchase and Assignment Agreement

On November 15, 2005, CCM and HIT entered into a Purchase and Assignment Agreement under which HIT conveyed the right, title, and interest in the Hefter Shell Design to CCM. (Def. Mot. Summ. J. SMF Ex. 2, Purchase and Assignment Agreement (the "Agreement")). The Agreement provided for a lump-sum payment of $350,000 for the assignment of the Hefter Shell Design and for royalties of 4.5% of all net sales of "any Product that incorporates the Shell Design." (*Id.* § 3.5). As relevant here, "Product" is defined under the Agreement to mean "a hockey helmet that incorporates the Shell Design." (*Id.* § 2.14). "Shell Design," in turn, is defined to mean "the design shown in [a schematic attached to the Agreement], including the ornamental design and technical features of the design, or any shell derived therefrom and substantially similar thereto." (*Id.* § 2.15).

##### a. Helmets Not in Dispute

After signing the Agreement, CCM developed a new line of hockey helmets called "Vector" based, in part, on the Hefter Shell Design. (Def. Mot. Summ. J. SMF ¶ 5). The

line encompassed multiple helmet models with different shell designs. (Martin Dep. 134–35). A CCM employee named Phillipe Martin was responsible designing the Vector line. (*Id.* at 91–92). Martin testified that for one set of Vector models, about 30% of the design was based on the Hefter Shell Design. (*Id.* at 135). For another set of Vector models, less than about 50% was based on the Hefter Design. (*Id.* at 134).

***2** CCM viewed the Vector line as a success. (Gibson Dep. 121). By 2012, about a third of National Hockey League players were wearing helmets from that line. (*Id.*). The parties agree that royalties are payable on the sale of any Vector helmets, and that CCM has paid HIT royalties for the sale of those helmets under the terms of the Agreement. (Def. Mot. Summ. J. SMF ¶ 6).

**b. Helmets in Dispute**

The dispute in this case centers on helmets developed after the Vector line: the Resistance line, the HT11K helmet, and the FitLite line. (*Id.* ¶ 7).

Phillippe Martin was also the lead designer on the Resistance line of helmets. (Martin Aff. ¶ 2). The development of that line began around 2010 and was completed in late 2013. (Gibson Aff. ¶ 2). One of CCM's express objectives in developing the Resistance line was to avoid paying HIT royalties on helmet sales. (Gibson Dep. 185–86). Martin testified that although there are some elements in common between the Resistance design and the Hefter Shell Design, including the placement of ventilation holes, those elements were not inspired by the Hefter Shell Design. (Martin Dep. 219). According to Martin, "the outer shell design of the Resistance helmets was not derived from [the Hefter Shell Design] or the design of any other then-existing hockey helmet. Put another way, neither [the Hefter Shell Design] nor the Vector shell designs were reused in the design of the Resistance outer shell." (Martin Aff. ¶ 3).

Another helmet designer employed by CCM, Sebastian Morin, was the lead designer on the HT11K helmet and the FitLite line of helmets, which includes the FL40, FL60, FL80, and FitLite 3DS models. (Morin Aff. ¶ 2). Like Martin, Morin contends that the designs of those helmets were not derived from the Hefter Shell Design or any Vector or Resistance helmet. (*Id.*¶ 3). He further contends that the HT11K, the FL40, FL60, and FL80 were derived from the shells of a helmet line called the 8K helmet, which had a design completed before November 2005. (*Id.* ¶ 3). He further contends that he designed the FitLite 3DS helmet model based on feedback he received from NHL star Sidney Crosby as to his preferences in a helmet. (*Id.* ¶ 4).

**c. Ball Report**

Roger M. Ball, HIT's expert witness, is a professor of industrial design at Georgia Tech University. (Docket No. 110, Ball Report Ex. B). He has more than thirty years of experience in industrial design, including as a designer and design consultant in the hockey industry. (*Id.*). He holds four United States patents on ice-hockey and snowboard helmets, and has authored articles on the design of protective headgear. (*Id.*).

In his expert report, Ball opined that the Hefter Shell Design has a "stealth fighter" look that "represents a significant departure from [CCM's] previous look of rounded, organic shapes." (Ball Report at 8). That look, he contends, has been maintained in the Resistance line, the HT11K, and the FitLite line. (*Id.* at 10). Ultimately, he concluded that although the helmets are "not identical," the Resistance line, the HT11K, and FitLite line of helmets are "derived from and are substantially similar to" the Hefter Shell Design. (*Id.* at 23–24).

**3. Alleged Spoliation of Evidence**

On September 22, 2014, HIT sent a letter to CCM demanding royalties for the sale of the Resistance line of helmets and informing CCM that it would take further action, including civil action, if not paid. (Pl. Mot for Sanctions Ex. L). The letter did not mention the HT11K or FitLite line. (*Id.*).

***3** When threatened with litigation, CCM's policy is to issue a "litigation-hold memorandum" instructing employees not to destroy relevant information. (Wexelblatt Dep. 39–40). Keith Wexelblatt is in-house counsel at CCM. (Wexelblatt Aff. ¶ 1). Wexelblatt testified that the memorandum instructs the relevant document custodians not to destroy any information, to put all relevant information to the side, and to not delete any

hard-copy or e-mail documents. (Wexelblatt Dep. 39). He also testified that he and other business leaders may issue verbal and written reminders concerning the memorandum as necessary. (*Id.* at 40).

After receiving HIT's letter, presumably in September or October 2014, Wexelblatt issued a litigation-hold memorandum to a number of employees involved in the development of the Resistance line. (Wexelblatt Aff. ¶ 4). The memorandum is not a part of the record in this case, as CCM has refused to produce the document based on a claim of privilege. Wexelblatt testified that he believed that the employees to whom the memorandum was issued complied with it by preserving the requested materials. (Wexelblatt Dep. 46–47). He testified that in order to ensure compliance, he spoke with some of the people to whom the memorandum was issued and with the information technology department, but could not remember with whom he spoke or what was said in those conversations. (*Id.* at 68–69). He did not take any other measures to ensure compliance with the memorandum. (*Id.* at 69).

CCM sent out an updated litigation-hold memorandum after the complaint and amended complaint were filed in early September 2015. (Wexelblatt Dep. 63; Wexelblatt Aff. ¶ 5). Like the letter, those pleadings only asserted claims for royalties on helmets in the Resistance line. (Docket No. 1; Docket No. 8).

On August 2, 2016, eleven months after the original complaint was filed, HIT notified CCM that it intended to add a claim for royalties on the sale of the HT11K and FitLite line of helmets. (Davidson Aff. ¶ 6). On August 23, 2016, HIT filed an assented-to motion for leave to file a second amended complaint adding those models to its claims, which was granted the same day. (Docket No. 43–44). At some point thereafter, CCM again updated its litigation-hold memorandum to include the additional models. (Wexelblatt Dep. 63).

Connie Cadovius was the CCM employee responsible for assembling documents concerning HIT's claims. (Cadovius Dep. 14). She testified that she independently assembled documents "from the archives," and also asked document custodians for both electronically-stored information and hard-copy documents. (*Id.* at 20, 30). The employees to whom the litigation-hold memorandum was issued did not produce any hard-copy documents responsive to it because, she was told, no such documents existed. (*Id.* 30–31).

**a. Electronically-Stored Information**

Around 2008, CCM changed the system employees used to send, receive, and store e-mail. (Wexelblatt Dep. 25). During the transition to the new e-mail system, stored e-mails that had been sent and received prior to the switch were destroyed. (*Id.*).

Also in 2008, CCM implemented an e-mail retention policy that allows employees to manage their e-mail storage. (*Id.* at 28). Under that policy, employees are permitted to store e-mails until their storage capacity runs out, after which they must delete messages to free up space. (*Id.*). CCM saves backup copies of e-mails for three months and then destroys them. (*Id.*). The e-mails of employees who have left the company are also destroyed three months after their exit. (Wexelblatt Aff. ¶ 3). For all other documents stored on employees' computers, employees are free to determine which documents to retain and how long to retain them. (*Id.*).

***4** Cadovius testified that at some point, she requested e-mail backups from the information technology department for two former employees who had not been identified as document custodians. (Cadovius Dep. 54–55). Those employees had left the company more than three months prior to CCM's receipt of HIT's September 22, 2014 letter. (Wexelblatt Aff. ¶ 8). Cadovius testified that a person in the department told her that "he had no email older than three months." (Cadovius Dep. 54–55).

Cadovius also testified that she went to the information technology department in 2016 to request e-mail backups for document custodians. (*Id.* at 59). She was told by an employee that, as to the document custodians she had identified, he "didn't have backup e-mails further than the policy required." (*Id.*). Cadovius did not know whether e-mails had been deleted. (*Id.* at 58).

According to Wexelblatt, after receiving the September 22, 2014 letter from HIT threatening litigation, he requested that CCM's information technology department take a "snapshot" of the e-mail mailboxes of the employees who had received the hold memoranda. (Wexelblatt Aff. ¶ 4). Those snapshots recorded a complete duplicate of

the content of the subject's e-mail mailbox, including the inbox, sent mail, deleted mail, and folders. (*Id.*).

**b. Document Destruction**

Laura Gibson has worked at CCM since 2006. (Gibson Aff. ¶ 1). She is a Canadian resident and works at the CCM office in Montreal. (Gibson Dep. 18). She was the product manager for the Resistance line and many of the helmets in the FitLite line. (*Id.* at 23–24). She was one of the employees who received the litigation-hold memorandum following the receipt of HIT's September 22, 2014 letter. (*Id.* at 44).

In her capacity as product manager, Gibson worked with salespeople, distributors, dealers, focus groups, and professional athletes to gather feedback on helmets. (*Id.* at 24). She kept notebooks in which, among other things, she recorded handwritten notes from some of those conversations. (*Id.* at 37). She describes the notebooks as "a running series of random notes regarding what [she] did, should do or might do." (Gibson Aff. ¶ 5).

During her time at CCM, Gibson has taken maternity leave twice; once from January 2013 to January 2014, and again from January 2015 to October 2015. (Gibson Dep. 19). In January 2013, at the time of her first maternity leave, she discarded all of her then-existing notebooks. (Gibson Aff. ¶ 6). She resumed taking notes in notebooks when she returned from that leave in January 2014. (*Id.*) She stated that it was her practice to throw notebooks away as she filled them. (Gibson Dep. 40). In addition, she cleaned out her desk at the start of her second maternity leave, and in the process discarded all of the notebooks that she had accumulated in 2014. (Gibson Aff. ¶ 6; Gibson Dep. 40). She did so even though she had received the litigation-hold memorandum only a few months previously. She testified that she discarded those notebooks because it "never occurred to [her] that anything [she] kept in [them] would be relevant to the claims for royalties that HIT has made." (Gibson Aff. ¶ 5).

In addition to those handwritten notes, Gibson stored briefs and other documents concerning the direction of helmet lines on her laptop. (Gibson Dep. 38). After she received the litigation-hold memorandum, she provided Wexelblatt with documents responsive to it, including e-mails. (Wexelblatt Dep. 56–58; Gibson Aff. ¶ 4). Gibson alone reviewed information on her laptop; no one from the legal department conducted an independent review to ensure that all responsive documents were produced. (Wexelblatt Dep. 57–58).

***5** Each time Gibson took maternity leave, CCM wiped her laptop clean. (Wexelblatt Aff. ¶ 6). According to CCM, under Canadian law, when a woman takes maternity leave she technically ceases her employment with the company and becomes employed by the government. (*Id.*). It is CCM's practice to destroy the files of all exiting employees, including those who take maternity leave. (*Id.*). Therefore, at the time the litigation-hold memorandum was issued, Gibson's laptop contained no information older than January 2014, because information from earlier in her tenure had been previously wiped clean. She testified that information she might have had on her laptop in 2014 would not have included any documents concerning the design or development of the Resistance helmet, because that was completed in 2013, prior to her first maternity leave. (Gibson Dep. 202). She did not foreclose the possibility that her laptop may have contained some information concerning the Resistance helmet; instead, she stated that she "might have had some stuff" but could not recall any specifics. (*Id.*).

**c. Supplemental Document Production**

In April 2016, counsel for HIT notified CCM that he was concerned that only a small number of documents had been produced in response to HIT's discovery requests. (Pl. Mot. Sanctions Ex. P). Counsel for CCM responded that HIT had received all of the documents that CCM had agreed to produce. (*Id.*).

In September 2016, HIT took the deposition of Laura Gibson. (Gibson Dep.). Both Wexelblatt and outside counsel for CCM, Shepard Davidson, learned for the first time at that deposition that Gibson had discarded her notebooks prior to leaving for maternity leave in January 2015. (Wexelblatt Aff. ¶ 7; Davidson Aff. ¶ 7).

Gibson also testified at her deposition that she had forwarded potentially relevant e-mails and documents to other CCM employees in the marketing department. (Davidson Aff. ¶ 8). In response to that testimony, Davidson instructed CCM to expand the search for e-

mails to employees in the marketing department. (*Id.*). Also in response to that testimony, Davidson instructed CCM to have Gibson and other employees review the e-mail mailbox snapshots that had been taken in the fall of 2014 to ensure that they had not missed any e-mails that were responsive to CCM's requests. (*Id.* ¶ 9).

As of the fall of 2016, the operative scheduling order in this case set a deadline for the close of fact discovery on November 29, 2016. (Docket No. 67). About one month prior to that deadline, on October 26, 2016, CCM made a supplemental production of a significant number of documents. On December 15, 2016, CCM produced some additional e-mails. (Pl. Mot. for Sanctions at 4).[2] CCM contends that it made those supplemental productions after expanding its search for documents in response to deposition testimony by Gibson (and others).

**B. Procedural Background**

On September 3, 2015, HIT filed the complaint in this action, which it amended on September 14. A second amended complaint was filed on August 23, 2016. The second amended complaint alleges five counts for breach of contract, breach of the duty of good faith and fair dealing, unjust enrichment, and seeks a declaratory judgment that it is owed royalties on the Resistance line, HT11K, and FitLite line helmets, and an accounting of unpaid royalties.

HIT has filed a motion for sanctions for spoliation of evidence alleging that CCM destroyed relevant documents.

**II. Analysis**

The scope of the documents at issue in this motion is relatively narrow. HIT contends that CCM destroyed documents in three categories: e-mails lost due to routine management of electronically-stored information; electronic documents stored on Gibson's laptop when it was wiped in December 2014; and Gibson's hard-copy notebooks.

**A. Electronically-Stored Information**

***6** The issuance of sanctions for loss of electronically-stored information is governed by Fed. R. Civ. P. 37(e). The present version of Rule 37(e), effective as of December 1, 2015, provides as follows:

> If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:
>
> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> (A) presume that the lost information was unfavorable to the party;
>
> (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
>
> (C) dismiss the action or enter a default judgment.

Fed. R. Civ. P. 37(e) (effective Dec. 1, 2015). The Advisory Committee Notes to the 2015 amendment to Rule 37(e) provide that the Court has "discretion to determine how best to assess prejudice in [a] particular case." Fed. R. Civ. P. 37(e) Advisory Committee Notes (2015 amendment).

The prior version of the rule, in effect at the time that this litigation was filed, provided that "[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good faith operation of an electric information system." Fed. R. Civ. P. 37(e) (effective until Nov. 30, 2015).[3]

In amending the Federal Rules of Civil Procedure in 2015, the Supreme Court provided courts with some discretion to choose which version of a rule to apply in cases that were pending at the time the change became effective. *See* 2015 U.S. ORDER 0017 (C.O. 0017) ("[T]he foregoing amendments to the Federal Rules of Civil Procedure shall take effect on December 1, 2015, and shall govern in all proceedings in civil cases thereafter commenced and, insofar as just and practicable, all proceedings then pending."). This case was brought in September 2015, only three months prior to the effective date of the amended rules. CCM did not file an answer until December 21, 2015. In light of the close proximity in time of the filing of the complaint and the effective date of the amendment,

it appears both just and practicable to apply the amended Rule 37 to this case.

***7** First, HIT contends that sanctions are warranted due to CCM's failure to suspend its policy of deleting e-mail backups every three months. However, HIT has not shown that any relevant e-mails were in fact destroyed. HIT points to the deposition testimony of Connie Cadovius as support for its claim; but although she stated that she had been told that there were no backups of e-mail older than three months, she also stated that she did not know whether e-mails had been deleted. According to CCM's in-house counsel Wexelblatt, all employees who were identified as document custodians had a snapshot taken of their e-mail mailboxes around the time that CCM received the September 22, 2014 letter from HIT threatening litigation. That contention is supported by the fact that CCM made a supplemental production of e-mails that apparently had been overlooked in 2014, but located when the e-mail snapshots were reviewed in 2016. While the record supports a conclusion that CCM's response to the document production request was very far from ideal, it does not support a finding that any relevant e-mails were actually destroyed.

Next, HIT contends that CCM should be sanctioned for failing to preserve information on Gibson's laptop. First, it appears that relevant evidence on Gibson's laptop was produced to CCM and preserved prior to being wiped. There is no basis for sanctions where information that was destroyed in one form is available in another form. *See Alexce v. Shinseki*, 447 Fed.Appx. 175, 178 (Fed. Cir. 2011) ("The routine destruction of duplicative documents does not present the risk of denying an adversary access to relevant information, which is what the doctrine of spoliation is directed to."). According to both Wexelblatt and Gibson, Gibson reviewed the information on her laptop prior to taking leave, located responsive documents, and provided them to Wexelblatt.

That does not, however, end the inquiry. In light of the fact that CCM employees found e-mails they had previously missed when they were asked to review the e-mail snapshots in 2016—and Wexelblatt's testimony that no one verified that Gibson produced all responsive documents prior to her leave—it is possible that CCM's review of information on Gibson's laptop was less than exhaustive. However, even if the Court assumed that CCM's cursory approach to document production resulted in Gibson's laptop being wiped prior to a thorough review, sanctions are inappropriate because there is insufficient evidence from which to find that CCM acted with the requisite intent, or that HIT will suffer prejudice.

First, there is no evidence that CCM wiped Gibson's laptop with the intent to deprive HIT of evidence. CCM had a policy to wipe information from the laptops of employees taking maternity leave. It had wiped Gibson's laptop when she took her first maternity leave. The evidence in the record does not support a finding that CCM acted in bad faith by wiping her laptop at the start of her second maternity leave in December 2014.

Second, there is insufficient evidence from which to infer that HIT would suffer prejudice if CCM's review of the information on Gibson's laptop was less than perfect. Again, when CCM wiped Gibson's laptop in December 2014, the laptop contained only information from the period between her maternity leaves: January 2014 to December 2014. At that time, CCM was under an obligation to preserve only information concerning the Resistance line of helmets. Gibson testified that the design of the Resistance line was completed in 2013 and that in December 2015, her laptop would not have contained anything concerning the development or design of the Resistance line. She did testify that she "might have had some stuff" concerning the Resistance line, but could not identify what documents she had, if any. Insofar as the Court infers that CCM missed some relevant documents on the margin prior to wiping Gibson's laptop, there is little evidence to support a finding that HIT was prejudiced as a result. [4]

***8** Accordingly, based on the record before the Court, no sanctions are appropriate against CCM for failure to preserve electronically-stored information pursuant to Rule 37(e).

**B. Notebooks**

The standard for finding spoliation of physical evidence, including the notebooks at issue here, is somewhat different from that articulated under Rule 37. Under the relevant standard, spoliation requires: "(1) an act of destruction; (2) discoverability of the evidence; (3) intent to destroy the evidence; and (4) occurrence of the act after commencement of litigation or, if before, at a time when

the party was on notice that the evidence might be relevant to potential litigation." *Gordon v. DreamWorks Animation SKG, Inc.*, 935 F. Supp. 2d 306, 313 (D. Mass. 2013).

Courts have inherent power to impose sanctions on parties that have spoliated evidence. *Chambers v. NASCO, Inc.*, 501 U.S. 32, 43–45 (1991). In determining what sanctions to apply upon a finding of spoliation, courts consider, among other things, whether a party acted in good faith or bad faith, and whether prejudice resulted from the destruction of evidence. *Townsend v. Am. Insulated Panel Co.*, 174 F.R.D. 1, 4 (D. Mass. 1997) (quoting *Mayes v. Black & Decker (U.S.), Inc.*, 931 F. Supp. 80, 83 (D.N.H. 1996)); *see also Collazo-Santiago v. Toyota Motor Corp.*, 149 F.3d 23, 29 (1st Cir. 1998) ("[O]f particular importance when considering the appropriateness of sanctions is the prejudice to the non-offending party and the degree of fault of the offending party"). In general, an adverse inference based on spoliation "usually makes sense only where the evidence permits a finding of bad faith destruction; ordinarily, *negligent* destruction would not support the logical inference that the evidence was favorable to the defendant." *United States v. Laurent*, 607 F.3d 895, 902 (1st Cir. 2010) (emphasis in original). However, "mere negligence in the destruction of evidence" can sometimes be "sufficient to merit sanctions." *Citizens for Consume v. Abbott Laboratories*, 2007 WL 7293758, at *7 (D. Mass. Mar. 26, 2007).

It is undisputed that Gibson destroyed her notebooks. It is also undisputed that she did so, at least in part, after CCM received HIT's September 22, 2014 letter and Gibson received the litigation-hold memorandum, placing her under an obligation to preserve all documents related to the Resistance line. According to her sworn affidavit, she threw notebooks away at the beginning of her second maternity leave because it "never occurred to [her] that anything [she] kept in [them] would be relevant to the claims for royalties that HIT has made." She also testified at her deposition that it was her practice to discard notebooks as she filled them and that she discarded notebooks at the beginning of her first maternity leave as well as her second leave. From that evidence, it is fair to infer that Gibson did not act with intent to deprive HIT of the notebooks by discarding them. Instead, her actions appear to be negligent, at worst.

It is far from clear that HIT suffered any prejudice due to the destruction of Gibson's notebooks. At the time they were discarded, Gibson was obligated to preserve only information concerning Resistance helmets. Like the information on her laptop, she had only notebooks from the 2014 calendar year, at which point the design and development of the Resistance line had been completed. Therefore, it is unlikely that the notebooks would have contained a substantial amount of information that was highly probative of CCM's liability.

**C. Conclusion**

***9** In light of the weak showing of prejudice and Gibson's lack of intent to deprive HIT of evidence, severe sanctions against CCM are not warranted. It appears that no probative electronically-stored information was destroyed. Some evidence may have been destroyed when the notebooks were discarded, but HIT will not suffer substantial prejudice as a result. Nonetheless, the combination of CCM's failure to preserve the notebooks, its somewhat lackadaisical approach to document production, and its aggressive document destruction policies has created substantial issues in this case. At a minimum, it has complicated the discovery process. Hefter's decision to bring this motion, although not ultimately successful, was an entirely reasonable response under the circumstances.

Accordingly, the sanction that the Court will impose is that CCM will be required to pay the reasonable attorneys' fees and costs HIT incurred in bringing this motion. *See In re Ethicon, Inc. Pelvic Repair Sys. Prod. Liab. Litig.*, 299 F.R.D. 502, 526 (S.D.W. Va. 2014) (imposing sanction of reasonable costs of bringing motion for sanctions for spoliation where party negligently lost relevant evidence). HIT may file an application for the reasonable attorneys' fees and costs it incurred in bringing this motion for sanctions for spoliation, along with any supporting documentation, within two weeks of the date of this order.

**III. Conclusion**

For the foregoing reasons, HIT's motion for sanctions for spoliation is GRANTED in part and DENIED in part. Specifically, the motion is granted to the extent that CCM shall pay to HIT the reasonable attorneys' fees and costs HIT incurred in bringing this motion for sanctions for spoliation. The motion is otherwise denied.

**So Ordered.**

**All Citations**

Slip Copy, 2017 WL 3317413

Footnotes

1 "Shell" is a term in common use that refers generally to the hard outer layer that is visible when a helmet is worn. Although the Agreement uses the term "Shell Design" to refer to the design at issue here, the Court, following the parties' lead, uses the term "Hefter Shell Design" to avoid confusion.

2 The parties have not provided the Court with sworn testimony concerning the number of documents produced in the supplemental production, but they appear to agree that the October production consisted of a substantial number of documents while the December production was more modest.

3 Courts interpreted the earlier version of Rule 37(e) to permit the imposition of sanctions only upon a finding that a party acted with a "culpable state of mind" in failing to preserve evidence, which included negligence and gross negligence. *See, e.g., Residential Funding Corp. v. Degeorge Fin. Corp.*, 306 F.3d 99, 113 (2d Cir. 2002). The current version of Rule 37(e)(2) provides for the possibility of severe sanctions where a court finds that a party acted with intent to destroy evidence, but rejects the imposition of sanctions under that provision where a party is found to be negligent or grossly negligent. *See* Fed. R. Civ. P. 37(e) Advisory Committee Notes (2015 amendments) (stating that the amended Rule 37(e)(2) "rejects cases such as *Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99 (2d Cir. 2002), that authorize the giving of adverse-inference instructions on a finding of negligence or gross negligence."). Where electronically-stored information is lost due to the negligence or gross negligence of a party, amended Rule 37(e)(1) permits only the imposition of sanctions that are "no greater than necessary to cure the prejudice."

4 The potential prejudice, if any, of the lost materials is necessarily framed by the nature of the proceeding. This is an action for breach of contract. The design of the helmets at issue is not a secret; whether the design was "derived from" the HIT design can be determined largely from a visual inspection.

**End of Document**

2016 WL 3538823
Only the Westlaw citation is currently available.
United States District Court,
N.D. Illinois, Eastern Division.

Daniel Martinez, Plaintiff,
v.
City of Chicago, et al., Defendants.

No. 14-cv-369
|
Signed 06/29/2016

**MEMORANDUM AND OPINION ORDER**

Robert M. Dow, Jr., United States District Judge

***1** Before the Court is Defendants' motion for partial summary judgment [174]. For the reasons set forth below, Defendants' motion [174] is denied. Also before the Court are Defendants' motions in limine 1–29 [140, 184, 185] and Plaintiff's motions in limine A–V [141], which are granted in part and denied in part as set forth below. As a housekeeping matter, Defendants' motion to file instanter an amended reply in support of Defendants' motion in limine no. 2 [163] is granted. This case remains set for a pretrial conference on July 6, 2016 at 1:15 p.m.

**I. Background**

On January 17, 2012, at approximately 3:45 p.m., non-Defendant officers Reynaldo Nunez and Joaquin Salazar, while on patrol and in their marked squad car, observed a vehicle run a stop sign and attempted to conduct a traffic stop. The offender, subsequently identified as Alberto Martinez (the brother of Plaintiff Daniel Martinez), exited his vehicle and began to run down an alley, tossing a revolver as he fled. After running through the alley and weaving through several streets, Alberto Martinez entered a residence located at the corner of Talman and 55th Street. Officer Nunez followed the suspect into the home, drawing his weapon upon entering. Officer Nunez searched the home but did not locate the suspect. Within minutes, additional police units arrived, and multiple officers began searching the area, including the interior and exterior of the home.

At some point, Defendant Officer Weber arrived on the scene to help search for "a male Hispanic with long hair, the last name Martinez," also described as a "male Hispanic with ponytail." [198, ¶ 5.] Sometime after entering the home, [1] Officer Weber encountered Plaintiff, who arguably matched the description of the suspect (*i.e.*, Plaintiff is also a Hispanic male, and he had long braided hair at the time [190, ¶ 17] ). Although the parties dispute the precise details of the interaction between Officer Weber and Plaintiff, Plaintiff said something along the lines of "Who the fuck are you," "What are you doing here," and "What the fuck is going on?" [198, ¶ 5.] Officer Weber, allegedly thinking that Plaintiff was, or might have been, the suspect in question, ordered him to lie down on the ground. [190, ¶ 19.] Plaintiff refused to comply with Officer Weber's orders and moved towards the door, prompting Officer Weber to restrain Plaintiff. At some point, Defendant Officer Chavez, who arrived separately on the scene, entered the room and assisted Officer Weber in restraining Plaintiff. The officers placed Plaintiff under arrest, handcuffed him, and placed him in a nearby squad car.

***2** One highly disputed issue is whether Defendants Weber and Chavez acted alone in arresting Plaintiff, or whether a third officer, Defendant Bogdalek, was also involved. Although Defendants deny that Officer Bogdalek was involved in the arrest, there is at least some evidence that a "blonde female" participated in the arrest, and Officer Bogdalek matches that description. The parties also note that Officers Weber and Bogdalek had prior run-ins with the Martinez brothers. More specifically, both officers were named defendants in a civil rights action in which both Alberto and Daniel Martinez were plaintiffs relating to an incident that occurred in September 2008. See *Martinez v. City of Chicago*, 09-cv-5938 (N.D. Ill.). At the time of Plaintiff's arrest, Defendant Bogdalek was still a named defendant in that case, but Officer Weber had been voluntarily dismissed.

At some point while Plaintiff was still in the squad car, Officer Bogdalek saw Plaintiff and said something along the lines of "That's not him. That's Danny." [190, ¶ 39.] About that time, other officers located the actual suspect, Alberto Martinez, hiding in a garbage can in the neighboring gangway. Despite confirmation that Alberto Martinez was the suspect in question, the officers kept Plaintiff in custody. Later that day, Officers Weber and Chavez filed sworn complaints against Plaintiff, each

charging him with resisting and obstructing a peace officer in violation of 720 ILCS 5/31-1(a). [190, ¶ 30.] Officer Bogdalek did not create a police report in connection with the arrests of either Martinez brother, nor was she mentioned in any of the other police reports relating to those arrests. [190, ¶¶ 42–43; 198, ¶ 18.]

## II. Analysis

### A. Summary Judgment

#### 1. Legal Standard

Summary judgment is proper where "the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c); see also *Sallenger v. City of Springfield, Ill.*, 630 F. 3d 499, 503 (7th Cir. 2010) (citing Fed. R. Civ. P. 56(c)(2) and noting that summary judgment should be granted "if the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law"). In determining whether summary judgment is appropriate, the court should construe all facts and reasonable inferences in the light most favorable to the non-moving party. See *Carter v. City of Milwaukee*, 743 F. 3d 540, 543 (7th Cir. 2014). Rule 56(a) "mandates the entry of summary judgment, after adequate time for discovery and upon motion, against any party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party would bear the burden of proof at trial." *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986)). Put another way, the moving party may meet its burden by pointing out to the court that "there is an absence of evidence to support the nonmoving party's case." *Id.* at 325.

To avoid summary judgment, the opposing party then must go beyond the pleadings and "set forth specific facts showing that there is a genuine issue for trial." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 250 (1986) (internal quotation marks and citation omitted). For this reason, the Seventh Circuit has called summary judgment the "put up or shut up" moment in a lawsuit—"when a party must show what evidence it has that would convince a trier of fact to accept its version of events." See *Koszola v. Bd. of Educ. of City of Chicago*, 385 F. 3d 1104, 1111 (7th Cir. 2004). In other words, the "mere existence of a scintilla of evidence in support of the [non-movant's] position will be insufficient; there must be evidence on which the jury could reasonably find for the [non-movant]." *Anderson*, 477 U.S. at 252.

#### 2. Conspiracy

***3** By way of background, on October 19, 2015, Defendants filed a motion for summary judgment seeking resolution of all claims in Plaintiff's complaint, which includes allegations of illegal search and seizure (Count I), false arrest (Count II), conspiracy (Count III), retaliation (Count IV), indemnification (Count V), and malicious prosecution (Count VI). However, discovery closed in this case on February 10, 2015 (*i.e.*, more than eight months before Defendants filed their motion for summary judgment), and, at the time of filing, this case was set for trial to begin approximately three months later, on January 11, 2016. During a status hearing on February 26, 2015, counsel for one of the Defendants raised the issue of dispositive motions and noted that if such a motion were filed, it would be limited to a single (unspecified) count. During that discussion, the Court proposed—and the parties accepted—a June 1, 2015 deadline for filing of any dispositive motions, recognizing that the trial date would be no sooner than November 1. Given that discussion, the Court concluded that Defendants' October 2015 motion for summary judgment was untimely, and struck it without prejudice. [See 134.] However, the trial date was later pushed back for unrelated reasons and, in an effort to streamline the issues at trial, the Court allowed briefing to proceed on Defendants' motion for summary judgment, but only as to Plaintiff's civil conspiracy claim (Count III). [172, at 1.] Defendants' renewed motion [174] is now before the Court.

A civil conspiracy is "a combination of two or more persons acting in concert to commit an unlawful act, or to commit a lawful act by unlawful means." *Scherer v. Balkema*, 840 F.2d 437, 441 (7th Cir. 1988). To establish conspiracy liability pursuant to § 1983, a plaintiff must establish that "(1) the individuals reached an agreement to deprive him of his constitutional rights, and (2) overt acts in furtherance actually deprived him of those rights." *Beaman v. Freesmeyer*, 776 F.3d 500, 510 (7th Cir. 2015) (citing *Scherer*, 840 F.2d at 442); see also *Hostrop v. Bd. of Jr. College Dist. 515*, 523 F.2d 569, 576 (7th

Cir. 1975) ("The doctrine of civil conspiracy extends liability for a tort * * * to persons other than the actual wrongdoer."). Summary judgment should not be granted "if there is evidence from which a reasonable jury could infer the existence of a conspiracy." *Id.* at 510–11 (citing*Cooney v. Casady*, 735 F.3d 514, 518 (7th Cir. 2013)). "Because conspiracies are often carried out clandestinely and direct evidence is rarely available, plaintiffs can use circumstantial evidence to establish a conspiracy, but such evidence cannot be speculative." *Id.* at 511 (citing *Williams v. Seniff*, 342 F.3d 774, 785 (7th Cir. 2003)).

Plaintiff argues that "a reasonable jury could conclude that the Defendants agreed to unlawfully continue Plaintiff's seizure in the absence of probable cause." [191, at 9.] According to Plaintiff's version of the facts, this agreement can be inferred because (a) Officers Weber and Bogdalek knew Plaintiff from a prior incident, and both were named defendants in a civil action brought by Plaintiff and his brother, (b) all three officers continued to detain Plaintiff despite knowing that he was innocent (*i.e.*, once police apprehended Plaintiff's brother and identified him as the suspect in question), and (c) Officers Weber and Chavez filed the same "false" charge against Plaintiff and both omitted Officer Bogdalek from their police reports despite evidence that she was involved in the arrest. Plaintiff says that "[t]he purpose of the continued unlawful seizure was to exact revenge on Plaintiff for his then[-pending] lawsuit while covering up the Defendants' illegal entry into the wrong home and seizure of the wrong person in the wrong place." [*Id.*] Further, Plaintiff claims that the conspiracy continued beyond Plaintiff's arrest in that Defendants "caused false and baseless charges against Plaintiff through false police reports, false and shifting testimony, false criminal complaints, and, in Bodgalek's case, the omission of any official report of her conduct at the scene in order to bolster her claim of minimal involvement and now catastrophic memory failure." [*Id.*]

Defendants' primary argument is that Plaintiff has failed to produce any "evidence that would permit a reasonable jury to conclude that a meeting of the minds had occurred." *Sow v. Fortville Police Dep't*, 636 F.3d 293, 305 (7th Cir. 2011). Temporally speaking, the "meeting of the minds" allegedly occurred when "Defendants agreed to unlawfully continue Plaintiff's seizure in the absence of probable cause." [191, at 9.] This would have been just after Defendants learned that Plaintiff's brother—*i.e.*, the actual suspect—had been apprehended, which happened while Plaintiff was handcuffed in a squad car. Plaintiff says that if there wasn't a conspiracy in place at this time, then the officers would have released Plaintiff. Instead, they conspired to keep Plaintiff in custody, now under an "obstruction of justice" theory.

***4** The Court concludes that there is sufficient evidence upon which a jury could infer a meeting of the minds. Defendants allegedly learned about the apprehension of Plaintiff's brother, the actual suspect, while Plaintiff was sitting handcuffed in a squad car. It is plausible to think that upon learning this news (whether from their fellow officers or from Officer Bogdalek, who allegedly recognized Plaintiff and stated that he was not the suspect), the officers who took part in the arrest (all three Defendants, according to Plaintiff) would have conversed about what to do with Plaintiff, and it is during this time period that they could have devised the scheme to charge Plaintiff with resisting and obstructing a peace officer. One relevant fact is that Plaintiff previously sued two of the officers, both of whom were allegedly involved in Plaintiff's arrest. Also important, if the jury believes that Officer Bogdalek actually was involved in the arrest (despite all three Defendants' testimony to the contrary), then the fact that her name was omitted from any police reports, including the reports of Officers Weber and Chavez, would imply some sort of concerted action amongst Defendants, further adding to the plausibility of Plaintiff's conspiracy theory. Moreover, as explained below in the motions in limine, Plaintiff is entitled to introduce evidence that Officer Bogdalek falsified a police report in a separate matter, and this attack on her credibility could also influence a jury in deciding whether a meeting of the minds occurred. While Plaintiff's conspiracy theory is built entirely on inference, there is enough inferential evidence to push Plaintiff's theory over the line from speculative to plausible.

One potential problem with this theory is that Defendants admit that when Officer Weber first confronted Plaintiff, the officer told Plaintiff to get down on the ground, and Plaintiff refused, saying something along the lines of "No, who the fuck are you?" while moving towards the door and refusing to comply with the officer's orders. [190, ¶ 18.] And when Officer Chavez entered the room, he saw Plaintiff struggling with Officer Weber as Weber attempted to restrain Plaintiff to keep him from leaving the room. [190, ¶ 20.] If the jury credits this version of the

facts, then it may conclude that Defendants Chavez and Weber potentially had probable cause to arrest Plaintiff for "resisting or obstructing a peace officer,"[2] which in turn would mean that the subsequent apprehension and identification of Plaintiff's brother as the suspect did not impact Defendants' right to continue holding Plaintiff in custody. On this view, the officers did not, as Plaintiff argues, "continue Plaintiff's seizure in the absence of probable cause," because the officers *had* probable cause to detain him separate and apart from any potential involvement in the preceding police chase. See *Powell v. City of Berwyn*, 68 F. Supp. 3d 929, 946 (N.D. Ill. 2014) ("Defendants had probable cause to arrest plaintiff on November 20, 2004, which negated plaintiff's false arrest claims and, therefore, precludes plaintiff from succeeding on his claim of conspiracy." (quoting *Southern v. City of Harvey, Ill.*, No. 2008 WL 4866337, at *3 (N.D. Ill. Jun. 4, 2008))). That being said, the parties did not adequately address whether the arresting officers had probable cause to arrest Plaintiff for resisting or obstructing a peace officer, and thus Plaintiff's conspiracy claim survives this hurdle as well.

Defendants also argue—relying on *Moore v. Morales*, 445 F. Supp. 2d 1000, 1012 (N.D. Ill. 2006)—that Plaintiff's conspiracy claim is unnecessarily redundant because Plaintiff is already suing Defendants for all of the potential predicate constitutional violations, including false arrest, malicious prosecution, and illegal seizure. To elaborate, "conspiracy is not an independent basis of liability in § 1983 actions." *Smith v. Gomez*, 550 F.3d 613, 617 (7th Cir. 2008). Instead, a § 1983 conspiracy claim is a vehicle by which individuals are held liable for some underlying constitutional violation, usually a means of "spreading the net of liability to additional persons," usually non-state actors.*Niehus v. Liberio*, 973 F.2d 526, 531–32 (7th Cir. 1992). However, "[a] plaintiff cannot prevail [on a conspiracy claim] if the defendants did not cause any injury above and beyond the torts that they allegedly conspired to commit." *Moore*, 445 F. Supp. 2d at 1012 (citing *Niehus*, 973 F.2d at 531–32); see also *Gramenos v. Jewel Cos., Inc.*, 797 F.2d 432, 435 (7th Cir. 1986) ("If the arrest was constitutionally unreasonable, then the police are liable under § 1983 without regard to the 'conspiracy,' and if not, not.").

***5** Plaintiff's only response as to why his conspiracy claim overcomes this "*Moore v. Morales*" hurdle, as the parties refer to it, is that "[u]nlike in *Moore*, Defendants here are obviously covering up the truth of who was involved," and "Defendants have offered nothing in the way of an explanation of how Chavez and Weber came to file the same false charge against Daniel, absent an agreement to file false charges." [191, at 10.] Setting aside the fact that there is a readily apparent explanation for this "conspiracy"—namely, that Officers Chavez and Weber filed the same charge against Plaintiff because they believed that Plaintiff committed the charged offense—Plaintiff's ability to introduce this conspiratorial evidence does not hinge on whether his conspiracy claim survives. See, *e.g.*, *Fairley*, 578 F.3d at 526 ("Plaintiffs appear to think that the [conspiracy] claim expands the scope of admissible evidence. But Fed. R. Evid. 801(d)(2)(E) (statement of coconspirator is not hearsay) applies whether or not the defendants are formally charged with a conspiracy.").

Defendants' argument that Plaintiff's conspiracy claim is entirely "subsumed in the other substantive tort claims" is not convincing either. [199, at 3.] To be sure, Plaintiff's conspiracy claim is somewhat amorphous. At first glance, it appears to relate only to a Fourth Amendment illegal seizure claim: "a reasonable jury could conclude that the Defendants agreed to unlawfully continue Plaintiff's seizure in the absence of probable cause." [191, at 9.] But Plaintiff also argues that Defendants carried out this conspiracy by "caus [ing] false and baseless charges against Plaintiff." [*Id.*] Arguably, then, Plaintiff's conspiracy theory could be read to include unlawful seizure, false arrest, and malicious prosecution claims. For the most part, Defendants are correct that these claims overlap with Plaintiff's other substantive counts: Count I (illegal search and seizure against Defendants Weber and Chavez), Count II (false arrest against Defendants Weber, Chavez, and Bogdalek), and Count VI (malicious prosecution against Defendants Weber, Chavez, and Bogdalek). However, there is one discrepancy: Plaintiff incorporates Defendant Bogdalek into his conspiracy-to-unlawfully-seize claim, but *does not* include her in the underlying unlawful-seizure claim. If the jury were to determine that Defendant Bogdalek made an agreement with the other officers to continue seizing Plaintiff's person despite knowledge that they lacked probable cause to do so, it could find Defendant Bogdalek conspiratorially liable for unlawfully seizing Plaintiff even if she did not actually seize him herself. And this logic is true for Plaintiff's other conspiracy theories as well. That is, if the jury concludes "that a meeting of the minds had

occurred and that the parties had an understanding to achieve the conspiracy's objectives," *Green v. Benden*, 281 F.3d 661, 666 (7th Cir. 2002), but determines that only one of the three Defendants falsely arrested or maliciously prosecuted Plaintiff, under Plaintiff's § 1983 conspiracy theory of liability, the jury could find the other Defendants liable for those claims as well. Accordingly, Defendants' motion for summary judgment [174] on Plaintiff's conspiracy claim (Count III) is denied.

**B. Defendants' Motions in Limine**

Before assessing the parties' motions in limine, the Court notes one overarching theme, which is its unwillingness to allow the parties to create unnecessary sideshows and mini-trials on issues of little relevance. The Court has, on several occasions, encouraged the parties to focus their arguments and to make efforts to streamline the issues at trial. Nonetheless, the parties have presented the court with almost 50 motions in limine—perhaps the most the Court has seen for a case of any size, and certainly the most for a case with a fact pattern this straightforward. These rulings, then, reflect the Court's effort to assist the parties in further refining the issues at trial.

**1. Motion to Bar Reference to Any Violation of Police Regulations**

***6** Defendants move in limine to bar Plaintiff from presenting any testimony, evidence, or argument relating to any violation of (or the existence of) any police department rules, policies, regulations, or general orders (*e.g.*, the Chicago Police Department General Orders). Defendants' motion is denied as overbroad.

Although "42 U.S.C. § 1983 protects plaintiffs from constitutional violations, not violations of * * * departmental regulations and police practices," *Scott v. Edinburg*, 346 F.3d 752, 760 (7th Cir. 2003), there is no categorical bar preventing parties from introducing such evidence. The general rule is that "any attempt to use violations of CPD General Orders or other policies and procedures as prima facie evidence of a constitutional violation is prohibited," but there "may be other circumstances in which this kind of evidence is admissible." *Gonzalez v. Olson*, 2015 WL 3671641, at *13 (N.D. Ill. June 12, 2015); see also *Thompson v. City of Chicago*, 472 F.3d 444, 454 (7th Cir. 2006) (evidence that an officer violated CPD's General Order regarding the use of force was not relevant in determining whether the officer violated the plaintiff's Fourth Amendment rights by using excessive force in apprehending him). The admissibility of such evidence hinges primarily on (a) whether the evidence is relevant, and (b) the extent to which the evidence might prejudice the jury. [3] See Fed. R. Evid. 401, 403. The proponent of such evidence "carries a heavy burden under FRE 401 and 403." *Gonzalez*, 2015 WL 3671641, at *13.

For example, Defendants anticipate that Plaintiff will attempt to introduce evidence that Defendant Weber violated a CPD General Order by failing to wear a lapel microphone during the incident in question. Plaintiff argues that Defendant Weber's failure to comply with this general order shows that he "intended to engage in wrongdoing or, at a minimum, deliberately left open the possibility that he or others might." [148, at 3.] Although this evidence sits near the outskirts of the relevance spectrum, it is arguably relevant to Plaintiff's conspiracy claim (*e.g.*, Defendant Weber intended to hide his conspiratorial agreement with his co-Defendants), and thus Plaintiff may be entitled to question Defendant Weber on this point. That being said, the Court will not permit a sideshow on ancillary evidentiary points such as this, and thus will defer ruling until trial. In addition, should the Court permit some minimal exploration of the lapel microphone issue, it will entertain objections should Plaintiff's presentation of this evidence become cumulative or prejudicial.

Accordingly, ruling on Defendants' motion is deferred. Should either party seek to introduce any evidence of this nature during trial, counsel should request a sidebar beforehand to allow the Court to rule on its admissibility outside of the presence of the jury.

**2. Motion to Bar Evidence of Defendants' Failure to Preserve Video**

Defendants move in limine to bar evidence or argument that the City of Chicago, including any of the named Defendants, failed to preserve the videos from Defendant Bogdalek's and Defendant Chavez's vehicles. Defendants' motion is granted.

***7** As an initial matter, Plaintiff has failed to establish that the video footage in question has any relevance to the issues in this case. See Fed. R. Evid. 401 (Evidence is relevant when it has "any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."). For example, this is not an excessive force case where video surveillance of an altercation might inform the jury regarding the officer's reasonableness. And unlike the audio recordings mentioned above that could have captured a "meeting of the minds" amongst Defendants, video footage would do little to elucidate the factual disputes here. For this reason, the Court is unwilling to permit what would surely be a lengthy sideshow regarding "missing evidence," especially considering the high potential for prejudice. Spoliation is a serious matter, and Plaintiff has not raised this issue in a substantive manner (*e.g.*, moved for sanctions or sought an adverse inference) until now, and Plaintiff offers no hard evidence, testimonial or otherwise, to support his theory. It is simply too late in the game to chart this course based solely on speculation, especially considering the low probative value of the evidence in question.

Plaintiff also notes that the allegedly spoliated video footage likely would have an audio component as well, which arguably would increase the potential relevance of this evidence. But this marginal increase in relevance does not outweigh the prejudicial impact that the impending mini-trial on spoliation would have. As discussed above, Plaintiff may be permitted to make his point about missing audio through limited questioning regarding lapel microphones.

### 3. Motion to Bar Evidence of the City's Customs, Policies, or Practices

Defendants move in limine to bar any evidence, argument, or innuendo regarding alleged policies, customs, or practices involving the City of Chicago—for example, evidence of a "code of silence" amongst police officers, or innuendo that "all cops lie." Defendants' motion is granted.

The evidence in question—*i.e.*, that related to the City's customs, policies, and practices— usually appears only in connection with a *Monell* claim against a municipality, not in cases concerning individual liability. See, *e.g.*, *Obrycka v. City of Chicago*, 2012 WL 601810, at *5–*9 (N.D. Ill. Feb. 23, 2012) (allowing "code of silence" *Monell* claims to proceed beyond the summary judgment stage). Here, the City of Chicago is a named Defendant only for indemnification purposes. In addition, any "code of silence" or "all cops lie" evidence would be unduly prejudicial and would constitute improper propensity evidence. See Fed. R. Evid. 403; *Cooper v. Dailey*, 2012 WL 1748150, at *4 (N.D. Ill. May 16, 2012).

That being said, Plaintiff is entitled to cross examine Defendants on their potential biases. See Fed. R. Evid. 607 ("Any party * * * may attack the witness's credibility."); *United States v. Abel*, 469 U.S. 45, 52 (1984) ( "Proof of bias is almost always relevant because the jury, as finder of fact and weigher of credibility, has historically been entitled to assess all evidence which might bear on the accuracy and truth of a witness' testimony."). Accordingly, to the extent that Plaintiff focuses on the Defendant officers involved in this case, he may explore the possibility that Defendants are biased because of their loyalty to one another, but *not* to other police personnel who are not involved in this case. See *Ford v. Bell*, 2012 WL 1416456, at *4 (N.D. Ill. Apr. 24, 2012) (precluding "code of silence" references generally, but allowing the plaintiffs to introduce evidence regarding bias with respect to the defendants in that case); *Maldonado v. Stinar*, 2010 WL 3075680, at *4 (N.D. Ill. Aug. 5, 2010) (same); *Betts v. City of Chicago*, 2011 WL 1837805, at *5 (same); *Caldwell v. City of Chicago*, 2010 WL 380696, at *3 (N.D. Ill. 2010) (same).

### 4. Motion to Exclude Evidence of Defendants' Prior Lawsuits, Etc.

Defendants move in limine to bar testimony, evidence, and argument regarding other civil lawsuits, arrests, and/or the disciplinary histories, and/or complaint registers against Defendants. In response, Plaintiff states that he agrees to refrain from introducing such evidence, except as it relates to Defendant Bogdalek's admitted perjury (discussed in detail below). Plaintiff also reserves his right to change his position to the extent that Defendants' testimony puts this evidence at issue. Accordingly, Defendants' motion is denied as moot. Should either party seek to introduce any evidence of this nature during trial, counsel should request a sidebar beforehand to allow the Court to rule on its admissibility outside of the presence of the jury.

**5. Motion to Bar Evidence of Defendant Bogdalek's Prior Misconduct**

***8** Defendants move in limine to bar Plaintiff from calling Defendant Bogdalek as an adverse witness to question her about her perjurious statements in an unrelated police incident not involving Plaintiff. Defendants' motion is denied.

The prior misconduct in question relates to a well-publicized incident where Officer Bogdalek testified untruthfully in a criminal proceeding relating to a 2010 robbery. According to a recent news account, "[w]hile under oath on the stand, [Bogdalek] told the courtroom she hadn't shown the liquor store owner—who was shot in the leg during the 2010 robbery—a photo spread with [the defendant's] picture prior to his arrest. In reality, she had shown the owner [the defendant's] photo, but the victim initially failed to identify [the defendant] as the assailant." CHICAGO SUN TIMES, *Accused of Perjury, Chicago Police Officer Resigns* (May 30, 2016), available at http://chicago.suntimes.com/news/accused-of-perjury-chicago-police-officer-resigns/. Bogdalek confessed her perjury after the release of a recording of a phone call that she had with her supervisor in which she mentioned that she had shown lineup photos to the liquor store owner shortly after the robbery. *Id.*

Federal Rule of Evidence 608(b) says that parties are entitled to inquire into specific instances of a witness's conduct on cross-examination if they are probative of the witness's character for truthfulness. Fed. R. Evid. 608(b). Perjuring oneself in a judicial proceeding is a paradigmatic example of such conduct, and there is no question that Defendant Bogdalek actually engaged in this conduct (she's admitted as much).

That being said, the Seventh Circuit has instructed that even if evidence of prior misconduct is relevant as to a witness's truthfulness, "[w]hat questions are allowed remains subject to 'the overriding protection of Rule 403,' which requires that their 'probative value not be outweighed by danger of unfair prejudice, confusion or issues, or misleading the jury.' " *United States v. Abair*, 746 F.3d 260, 263 (7th Cir. 2014) (quoting Fed. R. Evid. 608(b) Advisory Committee Note for 1972); see also *United States v. Seymour*, 472 F.3d 969, 971 (7th Cir. 2007) ("Rule 403 establishes the standard for the exercise of the judge's discretion in evidentiary matters, which of course includes cross-examination" under Rule 608(b)); *Thompson v. City of Chicago*, 722 F.3d 963, 977 (7th Cir. 2013) ("The scope of cross-examination under Rule 608 is subject to Rule 403 balancing, however."). Moreover, Plaintiff must accept the witness's answer in response to the impeaching question(s), and may not introduce extrinsic evidence to further impeach the witness. Fed. R. Evid. 608(b).

Defendants express concern that Plaintiff might use this credibility impeachment as propensity evidence: *i.e.*, if Officer Bogdalek lied in another court proceeding, she must be lying in this one. Fed. R. Evid. 404(b)(1). Defendants are correct: this evidence *is not* admissible pursuant to Rule 404(b), and *may not* be used as propensity evidence. Indeed, were this evidence not relevant to Officer Bogdalek's character for truthfulness, the Court would exclude it altogether as improper character evidence. But Rule 404 also explains that "[e]vidence of a witness's character may be admitted under Rules 607, 608, and 609." Fed. R. Evid. 404(a)(3). And the very "reason for allowing cross-examination under Rule 608(b) is to allow a party to attempt to cast doubt on a witness's reliability for telling the truth." *Varhol v. Nat'l R.R. Passenger Corp.*, 909 F. 2d 1557, 1567 (7th Cir. 1990). Thus, just because character evidence is inadmissible pursuant to Rule 404(b) does not make that same evidence categorically inadmissible pursuant to Rule 608 as well.

***9** However, Defendants raise a much more concerning basis for potential prejudice in that they continue to contend that Officer Bogdalek was *not* involved in Plaintiff's arrest, and that Plaintiff has exaggerated her role in this incident solely as a means of introducing this impeachment evidence to the jury. For the Court's purposes, the relevance of this impeachment evidence (Rule 401), its potential for prejudice (Rule 403), and the potential for harassment (Rule 601) are directly related to Officer Bogdalek's overall significance in this matter. Thus, although Defendants' motion is denied as a categorical matter (*i.e.*, Plaintiff is not barred from introducing this impeachment evidence altogether), Defendants are free to object to any gratuitous presentations of this evidence.

Importantly, Rule 608(b) expressly limits the introduction of bad-act impeachment to "cross-examination." Fed. R.

Evid. 608(b). That being said, the Advisory Committee on the Federal Rules of Evidence recently endorsed the practice of ignoring this "cross-examination" limitation:

> The Committee is aware that the Rule's limitation of bad-act impeachment to "cross-examination" is trumped by Rule 607, which allows a party to impeach witnesses on direct examination. Courts have not relied on the term "on cross-examination" to limit impeachment that would otherwise be permissible under Rules 607 and 608. The Committee therefore concluded that no change to the language of the Rule was necessary in the context of a restyling project.

Fed. R. Evid. 608(b) Advisory Committee Note, 2011 Amendment. At least one treatise has disagreed with the Committee, arguing that impeachment with bad-act evidence on direct examination "probably should not be allowed" as it would permit a direct examiner to "call an adverse or hostile witness merely for the purpose of producing the unfairly prejudicial effects of specific-instances evidence," which "could undermine accurate fact-finding, waste time, and unnecessarily harass the witness." 28 Victor James Gold, FEDERAL PRACTICE & PROCEDURE EVIDENCE § 6119 (2d ed. 2016). While this is a valid point, the countervailing concern is that a party could hide an impeachable witness by refusing to call him or her and instead relying on the opposing party to call the witness, thereby denying the opposing party of its opportunity to "cross-examine" that witness. That is particularly relevant here where the party in question is a named Defendant. Absent binding authority on this issue, the admissibility of this evidence falls within the Court's broad discretion on evidentiary matters. Here, the Court exercises that discretion in allowing Plaintiff to question Defendant Bogdalek about her prior misconduct on direct examination, although (1) that questioning is likely to be strictly limited and closely controlled and (2) Defendants are free to object should Plaintiff's questioning become irrelevant, harassing, or unduly prejudicial. See Fed. R. Evid. 401, 403, 601, 611.

Finally, Defendants argue that Plaintiff plans to call Officer Bogdalek "simply to maximize and dramatize her assertion of Fifth Amendment privilege." [140, at 9.] While the Court is sensitive to the potential prejudice of a party seeking to dramatize a Fifth Amendment invocation, see *Evans v. City of Chicago*, 513 F.3d 735, 740 (7th Cir. 2008), that is not reason enough to preclude this line of questioning entirely. It is not even clear that Officer Bogdalek will invoke the Fifth Amendment on the stand. But however Officer Bogdalek responds to Plaintiff's questioning, Plaintiff must take her answer. "That expression does not mean that [Plaintiff] may not press further to extract an admission, for instance, by reminding the witness of the penalties for perjury." *McCormick on Evidence*, § 41. But "[i]t is improper to enquire whether the witness was 'fired,' 'disciplined,' or 'demoted' for the alleged act [because] those terms smuggle into the record implied hearsay statements by third parties who may lack personal knowledge." *Id.* Understanding this limitation, and those imposed by Rules 401, 403, and 601, Plaintiff is entitled to question Officer Bogdalek about her prior misconduct as a means of impeaching her credibility. [4]

### 6. Motion to Bar Reference to the State's Attorney's Conduct

***10** Defendants move in limine to bar reference to a "long running dispute" between Plaintiff's counsel and the Cook County State's Attorney's Office over the destruction of court documents, which resulted in sanctions against the office. See *Martinez v. City of Chicago*, Case No. 09-cv-5938, Dkt. 232 (N.D. Ill. Nov. 20, 2014). The destruction of the criminal file in an unrelated criminal matter is irrelevant to this lawsuit, would create an unnecessary sideshow, and would unduly prejudice Defendants. See Fed. R. Evid. 403, 404(b). Defendants' motion is granted.

### 7. Motion to Bar "Code of Silence" Evidence

Defendants move in limine to bar testimony, evidence, or argument that police officers lie, conspire, cover up, or otherwise maintain a "code of silence" or "blue wall" to protect their fellow officers. Defendants' motion is granted.

As stated in response to Defendants' motion in limine #3, any "code of silence" or "all cops lie" evidence would be unduly prejudicial and would constitute improper

propensity evidence. See Fed. R. Evid. 403; *Cooper v. Dailey*, 2012 WL 1748150, at *4 (N.D. Ill. May 16, 2012). However, Plaintiff is entitled to cross examine Defendants on their potential biases. See Fed. R. Evid. 607 ("Any party * * * may attack the witness's credibility."); *United States v. Abel*, 469 U.S. 45, 52 (1984) ("Proof of bias is almost always relevant because the jury, as finder of fact and weigher of credibility, has historically been entitled to assess all evidence which might bear on the accuracy and truth of a witness' testimony."). Accordingly, to the extent that Plaintiff focuses on the Defendant officers involved in this case, he may explore the possibility that Defendants are biased because of their loyalty to one another, but *not* to other police personnel who are not involved in this case. See *Ford v. Bell*, 2012 WL 1416456, at *4 (N.D. Ill. Apr. 24, 2012) (precluding "code of silence" references generally, but allowing the plaintiffs to introduce evidence regarding bias with respect to the defendants in that case); *Betts v. City of Chicago*, 2011 WL 1837805, at *5 (same); *Maldonado v. Stinar*, 2010 WL 3075680, at *4 (N.D. Ill. Aug. 5, 2010) (same); *Caldwell v. City of Chicago*, 2010 WL 380696, at *3 (N.D. Ill. 2010) (same).

**8. Motion to Bar Evidence of Misconduct by Non-Defendants**

Defendants move in limine to bar testimony, evidence, or argument about the conduct of police officers in Plaintiff's (and his brother's) prior interactions with the Chicago Police Department. Defendants' motion is granted.

Defendants anticipate that Plaintiff or his family members intend to testify as to some or all of the following incidents: (1) the September 23, 2008 incident that gave rise to Case No. 09-cv-5938, (2) an October 2009 incident where Daniel and Vanessa Martinez claim they were verbally abused by other Chicago police officers; (3) testimony by Sofia Martinez that an unidentified officer told her that if she didn't open the door, he could still open it with his gun; (4) the opinion of various Martinez family members that police frequently drive by their home to harass them, and (5) the threat to Vanessa Martinez by an unknown officer that the officer would shoot Plaintiff's dog. These alleged acts of misconduct are irrelevant to this lawsuit, especially considering that, apart from the 2008 incident, they do not involve any of the named Defendants in this lawsuit. The introduction of these alleged facts would create an unnecessary sideshow and would unduly prejudice Defendants. See Fed. R. Evid. 403, 404. Plaintiff's arguments to the contrary are unavailing.

***11** Act #3 arguably is relevant because it relates to the incident it question, namely the officers' entry into the Martinez home(s) while they were pursuing Alberto Martinez. Plaintiff argues that the officer's threat "is relevant evidence of lack of consent," and while that may be true, consent to entry is not a contested issue in this case [5] (and arguably not even a relevant issue), and the introduction of an incendiary comment by a non-Defendant officer within this context most certainly is irrelevant and unduly prejudicial. See Fed. R. Evid. 401, 403. Thus, while Vanessa Martinez may testify as to what she witnessed on the day of Plaintiff's arrest in this matter, the Court will entertain objections to the scope of her testimony should it become cumulative or focus on issues irrelevant to this lawsuit, especially testimony meant to cast non-Defendant officers in a bad light. This applies equally to Plaintiff's allegations that an unknown officer threatened to shoot Plaintiff's dog.

**9. Motion to Bar Evidence of Unrelated Police Misconduct**

Defendants move in limine to bar testimony, evidence, or argument regarding allegations of police misconduct by officers unrelated to this incident—namely, highly-publicized incidents involving Chicago Police Officers. Any such evidence is irrelevant and highly prejudicial. Fed. R. Evid. 403; *Rodriguez v. Cervantes*, 2009 WL 3460100, at *2 (N.D. Ill. Oct. 20, 2009) (granting a similar motion); *Morrow v. City of Chicago*, 2011 WL 494577, at *1 (N.D. Ill. Feb. 7, 2011) (same). Defendants' motion is granted.

Plaintiff should tread lightly when making "generalized arguments about the way police dishonesty and misconduct affects society." [148, at 15.] Plaintiff claims that such arguments are relevant to his claim for punitive damages, but punitive damages are intended "to punish *a defendant* for *his* conduct," [6] and thus invoking a broader concept of general police dishonesty would be inappropriate. While punitive damages are intended to serve as an example or warning to other officers, the "example" is the defendant's wrongdoing. Thus, Plaintiff's counsel may argue that punitive damages are appropriate

to serve as an example to other officers that they should not do *what Defendants did in this case*, but Plaintiff may not reference "police dishonesty and misconduct" generally—such arguments are irrelevant and highly prejudicial. Fed. R. Evid. 401, 403.

**10. Motion to Exclude Evidence of Case No. 09-cv-5938**

Defendants move in limine to exclude evidence or argument regarding Case No. 09-cv-5938, the aforementioned civil rights action brought by multiple plaintiffs, including Alberto and Daniel Martinez, relating to an incident from September 2008. Defendants' motion is granted.

To be clear, Defendants do not dispute that the parties may elicit testimony (or stipulate) that, on January 17, 2012, Daniel and Alberto Martinez were plaintiffs in a civil lawsuit that included Officer Bogdalek as a defendant arising from an incident that took place in September 2008, and that Officer Weber had also been a defendant in that case prior to being voluntarily dismissed by the plaintiffs. All other information about that lawsuit—including the claims raised, the resolution of the case, the settlement amounts, and the attorneys' fees—is irrelevant and unduly prejudicial. Fed. R. Evid. 401, 403, 404.

Plaintiff argues that, in order to prove his retaliation claim (in which he alleges that Defendants' retaliated against him because he filed the 2009 lawsuit), he should be able to testify that he obtained a judgment against the City of Chicago to show that his prior lawsuit was meritorious. The Court is not persuaded. The City of Chicago—which is not a Defendant in this lawsuit for liability purposes—settled the 2009 lawsuit without admitting liability. In addition, Plaintiff fails to explain how the merit of the claims in the 2009 lawsuit impacts his ability to establish his retaliation claim here. See, *e.g.*, *Springer v. Durflinger*, 518 F.3d 479, 483 (7th Cir. 2008) ("To prevail on their § 1983 retaliation claim, [plaintiffs] need to prove (1) that they were engaged in constitutionally protected speech; (2) that public officials took adverse actions against them; and (3) that the adverse actions were motivated at least in part as a response to the plaintiffs' protected speech."); Fed. R. Evid. 401. But even if the resolution of the 2009 lawsuit were relevant to some degree, that relevance would be outweighed by the prejudice to Defendants, as evidence of a judgment against the City of Chicago would imply some prior wrongdoing or admission of guilt for Defendants. See Fed. R. Evid. 403, 404.

**11. Motion to Bar Evidence Regarding IPRA Investigations**

***12** Defendants move in limine to bar evidence regarding the Independent Police Review Authority ("IPRA") investigations stemming from any and all complaints from the Martinez family. Plaintiff does not oppose this motion. Defendants' motion is granted.

Any testimony or evidence relating to the IPRA investigations is excluded, except for impeachment purposes based on prior inconsistent statements. More specifically, if Plaintiff wishes to impeach an officer based on a statement that appears in an investigation report, he can do so, but Plaintiff is precluded from mentioning the origins of the prior inconsistent statement (*i.e.*, Plaintiff cannot mention that the prior inconsistent statements were made in connection with any investigation). See *Norton v. Schmitz*, 2011 WL 4984488, at *1 (N.D. Ill. May 27, 2011) ("[W]hen impeaching a witness using an IPRA statement, the attorney shall refer to the statement as one made 'in another proceeding'; the attorney shall not mention 'IPRA' or 'investigation.' ").

**12. Motion to Bar Evidence of Co-Conspirator Statements**

Defendants move in limine to bar Plaintiff from presenting evidence and arguments in support of a conspiracy claim until they satisfy Fed. R. Evid. 104 and Seventh Circuit law governing the admissibility of co-conspirator declarations. Plaintiff responds that he "does not understand this motion," claiming that the alleged co-conspirators' statements will be admissible as statements by a party opponent pursuant to Fed. R. Evid. 801(d)(2)(E), and that he is not aware of any other co-conspirator statements that will be offered at trial. Defendants' motion is denied. The Court is aware of the admissibility standards for statements by a party opponent and for statements of a co-conspirator,[7] and to the extent that Plaintiff attempts to admit statements under the latter exception, Defendants are free to object and hold Plaintiff to his burden.

### 13. Motion to Bar Evidence Regarding Plaintiff's Criminal Acquittal

Defendants move in limine to bar any evidence, argument, or innuendo as to why or how Plaintiff was acquitted of the charged offenses from his January 17, 2012 arrest. As Defendants note, these details of Plaintiff's criminal proceeding are (for the most part) irrelevant to this lawsuit, and their introduction would present a risk of prejudicing the jury as to the merits of Plaintiff's claims. Fed. R. Evid. 401, 403. However, Defendants concede that Plaintiff's acquittal is relevant to establish the "termination of the proceeding in favor of the plaintiff" element of an Illinois malicious prosecution claim, *Swick v. Liautaud*, 662 N.E.2d 1238, 1242 (Ill. 1996), and are willing to stipulate to this fact. Defendants' motion is provisionally granted. The parties are directed to work together to try reaching a stipulation on this issue and to advise the Court at the next pretrial conference whether they have been successful in that endeavor.

### 14. Motion to Bar Plaintiff from Alleging Physical Injury

***13** Defendants move in limine to bar Plaintiff from testifying as to any injuries that he suffered as a result of his interactions with Defendants surrounding his January 17, 2012 arrest— specifically Plaintiff's claim that he suffered slight wrist pain from being handcuffed—arguing that physical injuries are irrelevant to any of Plaintiff's claims (*e.g.*, Plaintiff does not allege an excessive force claim). Defendants' motion is denied. Although this evidence is not directly related to any particular claims in this case, it is still part of the narrative structure of the event in question. Defendants are free to raise specific objections at trial.

### 15. Motion to Bar Evidence or Argument of Alleged Racial Motivation

Defendants move in limine to bar evidence or argument that Defendants' actions towards Plaintiff were racially motivated. Although racial bias could be relevant to a claim of false arrest, there is no evidentiary basis for introducing allegations of racial animus into this trial, and Plaintiff does not argue otherwise. In addition, " '[a]ppeals to racial passion can distort the search for truth and drastically affect a juror's impartiality.' " *Dyson v. Szarzynski*, 2014 WL 7205591, at *8 (N.D. Ill. Dec. 18, 2014) (quoting *United States v. Doe*, 903 F.2d 16, 25 (D.C. Cir. 1990)); see also Fed. R. Evid. 403. Defendants' motion is granted.

### 16. Motion to Bar Undisclosed Witnesses

Defendants move in limine to bar Plaintiff from presenting witnesses at trial who were either not disclosed in Plaintiff's Rule 26 disclosure or were improperly disclosed, specifically: Lillian Ramos, ASA Mary McClellan, Darryl Smith, Shaniece Neighbors, Jeffrey McReynolds, and Samantha Acuff. In response, Plaintiff says that the only witnesses that he may call are Lillian Ramos and ASA Mary McClellan.[8] Regarding Lillian Ramos (Plaintiff's girlfriend), the parties provided supplemental briefing on the admissibility of her testimony, as reflected in Defendants' motion in limine #28, which the Court addresses below.

### 17. Motion to Bar References to Officers Not Having a Search Warrant

Defendants move in limine to exclude testimony that the officers failed to obtain a search warrant prior to entering the Martinez residence(s). Defendants' motion is denied. The terms upon which Defendants entered the Martinez residence(s) are relevant to Plaintiff's wrongful search claim. Plaintiff can ask the officers if they obtained a search warrant prior to entering the home, and Defendants can follow-up on cross-examination if necessary. The parties may suggest a jury instruction on the "hot pursuit" doctrine if they wish.

### 18. Motion to Bar Reference to the City's Indemnification Obligations

Defendants move in limine to bar Plaintiff from arguing or introducing evidence that the Defendant Officers may be indemnified by their employer, the City of Chicago, for any portion of a judgment that may be entered against them. Defendants' motion is provisionally granted.

"In the general case courts exclude evidence of indemnification out of a fear that it will encourage a jury to inflate its damages award because it knows the government—not the individual defendants—is footing the bill." *Lawson v. Trowbridge*, 153 F.3d 368, 379 (7th Cir. 1998); see also *Kemezy v. Peters*, 79 F.3d 33, 37 (7th Cir. 1996) ("When the defendant is to be fully indemnified, such evidence, far from being required, is inadmissible"). However, if a defendant who benefits from a right to indemnification nevertheless claims an inability to pay damages, the defendant is deemed to have "opened the door" to evidence of the statutory entitlement to indemnification. *Gonzalez v. Olson*, 2015 WL 3671641, at *7 (N.D. Ill. June 12, 2015) ("Evidence of indemnification is generally inadmissible, so if Defendants do not plead poverty as to punitive damages, Plaintiff may not introduce evidence of indemnification for compensatory damages. But if Defendants plead poverty as to punitive damages, they open the door for Plaintiff to offer evidence of indemnification as to compensatory damages.") (citing *Betts v. City of Chicago*, 784 F. Supp. 2d 1020, 1030–31 (N.D. Ill. 2011)). Thus, evidence of indemnification is inadmissible unless Defendants open the door by injecting any of the Defendant Officers' personal financial circumstances into the case. If Defendants choose to "apprise the jury of the fact that the individual officers will have to bear [punitive] damages out of their own pockets," then "fairness would dictate that the jury also be informed of the true situation (indemnification) as to compensatory damages," *Galvan v. Nordberg*, 2006 WL 1343680, at *2 (N.D. Ill. May 10, 2006), subject to an appropriate limiting instruction that "Defendants' finances address punitive damages only." *Townsend v. Benya*, 287 F. Supp. 2d 868, 874 (N.D. Ill. 2003).

### 19. Motion to Bar Evidence Regarding Questioning by City Attorneys

***14** Defendants move in limine to bar evidence, argument, or innuendo regarding the witnesses' communications with counsel relating to this matter. As an example, Defendants suggest that Plaintiff's counsel likely will question a police sergeant who was a defendant in the 2009 case about the fact that he contacted his attorney the day after the arrest of Daniel Martinez. Another example would be referencing attorney–client meetings to imply that a witness's change in testimony was influenced by the attorney (*i.e.*, the attorney instructed the witness to change his or her story). Defendants seek to avoid any implication that their witnesses contacted attorneys because they knew that they had done something illegal, or that the witnesses changed their testimony after meeting with their attorneys. Defendants' motion is granted.

The example of asking a witness when he or she met with an attorney to imply that the witness was aware of his or her wrongdoing presents a potential for prejudice that far outweighs any potential relevance of that evidence. See Fed. R. Evid. 403. Moreover, questioning a witness as to why he or she met with an attorney following Daniel Martinez's arrest would open the door to discussions of the Chicago Police Department's history with the Martinez family (*e.g.*, the testifying officer might say that he or she contacted his or her attorney knowing that the Martinez family is litigious), and the Court will not allow a matter of such little relevance to open the door to that rabbit hole.

As to the second example, arguing (or even implying) that a witness's change in testimony is the byproduct of attorney malfeasance is a serious accusation, and would be highly prejudicial absent credible evidence substantiating such a claim. Plaintiff is entitled to impeach witnesses with prior inconsistent statements, but cannot argue that the inconsistencies stem from attorney misconduct.

Plaintiff has failed to articulate any instance in which it would be relevant and/or not unduly prejudicial to elicit testimony regarding attorney–client communications. Accordingly, Defendants' motion is granted.

### 20. Motion to Bar Argument that the Jury Should "Send a Message"

Defendants move in limine to bar any argument that the jury should "send the City a message" with its verdict. Defendants' motion is granted.

Because the jury will not be resolving any claims against the City of Chicago in this case (the City is a named Defendant only for indemnification purposes), arguments regarding the City's financial role—whether as an indemnitor or as an independent wrongdoer—are irrelevant. Fed. R. Evid. 401. These arguments are also highly prejudicial because they invoke the City's

"deep pockets" and they imply that there is a systemic, municipal-wide problem, and that Defendants are a part of it. See Fed. R. Evid. 403. Plaintiff does not object to Defendants' position. [148, at 21.] Regardless, any such arguments are not permissible. See *Betts v. City of Chicago*, 784 F. Supp. 2d 1020, 1033 (N.D. Ill. 2011) ("[Plaintiff] is barred from any argument that the jury should 'send a message' to the City of Chicago.").

However, Plaintiff says that instead of arguing that the jury should send a message to the City, he "intends to argue that the jury should send a message *to the police department* that is sorely needed, as permitted by the jury instruction." [148, at 21 (emphasis added).] Plaintiff is referring to the pattern jury instruction on punitive damages, which says that the assessment of punitive damages is meant to "serve as an example or warning to Defendant *and others* not to engage in similar conduct in the future." Seventh Circuit Pattern Jury Instruction § 7.24 (emphasis added). The "others" in this scenario are other police officers, *not* the police department itself. Invoking the department is tantamount to invoking the City itself, creating the same "deep pockets" concern. More importantly, Plaintiff seemingly wants to use the potential for punitive damages to comment on his perceived faults with the Chicago Police Department. This is highly inappropriate. As the Court explained in response to Defendants' motion in limine #9, punitive damages are intended "to punish *a defendant* for *his* conduct," *id.* (emphasis added), and thus invoking a broader concept of general police dishonesty would be inappropriate. While punitive damages are intended to serve as an example or warning to other officers, the "example" is the defendant's wrongdoing. Thus, Plaintiff's counsel may argue that punitive damages are appropriate to serve as an example to other officers that they should not do *what Defendants did in this case*, but Plaintiff may not air his grievances with the Chicago Police Department generally —such arguments are irrelevant and highly prejudicial. Fed. R. Evid. 401, 403.

***15** To be clear, Plaintiff is entitled to ask the jury to send a message, in the form of an award of punitive (not compensatory) damages, to Defendants or to other police officers generally. See *Case v. Town of Cicero*, 2013 WL 5645780, at *10 (N.D. Ill. Oct. 16, 2013) ("Courts do allow plaintiffs to ask juries to 'send a message' to deter future misconduct by police officers by assessing punitive damages."); *Bruce v. City of Chicago*, 2011 WL 3471074, at *6 (N.D. Ill. July 29, 2011) ("Plaintiff will be permitted to argue that he is attempting to deter Defendant officers and other Chicago police officers from future misconduct.").

### 21. Motion to Bar References to "City" Attorneys

Defendants move in limine to bar Plaintiff from making any reference to certain Defendants' attorneys or any of the parties as "Corporation Counsel," "Assistant Corporation Counsel," "The City lawyers," "The City," or similar names and/or terms. References such as these would unduly prejudice Defendants by associating them with the "deep pockets" of the municipality, and would confuse the jury as to the City's role (or lack thereof) in this litigation. Fed. R. Evid. 403. Defendants' motion is granted.

### 22. Motion to Bar Evidence that Witnesses Are Paid to Testify

Defendants move in limine to bar any implication or testimony that Chicago Police Department personnel are being paid by the City of Chicago to appear in court and testify. Defendants' motion is provisionally granted.

The probative value, if any, of evidence that police personnel are being paid their normal wage to appear in court is outweighed by the potential prejudice of that argument (*i.e.*, that the officers' testimony is biased in favor of the City). Fed. R. Evid. 403. Although Plaintiff does not allege that officers are paid *more* than their standard wage (*i.e.*, an overtime wage) to testify in court, such evidence would be relevant to show bias. See *Betts v. City of Chicago*, 784 F. Supp. 2d 1020, 1029 (N.D. Ill. 2011). Plaintiff can ask CPD personnel whether they are being paid *more than* their normal wage to testify and, if they are, Plaintiff can argue regarding the officers' potential bias. Plaintiff cannot elicit testimony that testifying CPD personnel are being paid *in general*, or in accordance with their normal wage, nor can Plaintiff argue that being paid a normal wage to testify is evidence of bias. See *Id.* ("[Plaintiff] is barred from any argument or testimony that Chicago Police Department personnel are being paid any amount less than or equal to the wages they are normally paid to do their jobs as compensation for appearing in court and testifying, (2) [Plaintiff], however,

may argue or elicit testimony to show that Chicago Police Department personnel are being paid *more* than their normal wage to appear in court or testify since such evidence would be probative of those employees' bias."). To be sure, any questioning of this issue should be very brief; Plaintiff may make the point, but may not belabor it.

**23. Motion to Bar Witness Communications During Testimony**

Defendants' move in limine to bar attorneys and parties from conferring or speaking with any witness about that witness's testimony while that witness is still under oath to provide sworn testimony. Plaintiff does not object to this motion. Defendants' motion is granted.

**24. Motion to Bar Evidence of Plaintiff's "Good" Character**

Defendants move in limine to bar evidence or argument as to Plaintiff's "good" character (*e.g.*, "bolstering" of Plaintiff's character). Defendants' motion is premature, and thus is denied. Defendants may raise this objection at trial.

***16** " 'Bolstering' is the practice of offering evidence solely for the purpose of enhancing a witness's credibility before that credibility is attacked. Such evidence is inadmissible because it 'has the potential for extending the length of trials enormously, * * * asks the jury to take the witness's testimony on faith, * * * and may * * * reduce the care with which jurors listen for inconsistencies and other signs of falsehood or inaccuracy." *United States v. Lindemann*, 85 F.3d 1232, 1242 (7th Cir. 1996) (quoting *United States v. LeFevour*, 798 F.2d 977, 983 (7th Cir. 1986)). But once a witness's credibility has been attacked, "the non-attacking party is permitted to admit evidence to 'rehabilitate' the witness." *Id.*

Because Defendants have not articulated any specific concerns, the most Court can say at this point is that, upon objection by either party, the Court will enforce these standards regarding bolstering and rehabilitating witnesses.

**25. Motion to Bar Witnesses from Making Credibility Determinations**

Defendants move in limine to bar any witness from offering an opinion as to the credibility or accuracy of other witness's testimony or statements. Plaintiff does not oppose this motion. Defendants' motion is granted.

**26. Motion to Exclude Commentary on Missing Witnesses or Evidence**

Defendants move in limine to bar comment regarding Defendants' decision not to call a particular witness or not to present certain evidence. Confusingly, however, Defendants' argument in support of this motion relates to their request that the Court bar Plaintiff from introducing a video taken by the dash camera in Defendant Weber's vehicle. Then, in their reply brief, Defendants argue that Plaintiff should be barred from arguing that Defendants' spoliated evidence.

Breaking this down, Defendants' motion is granted as to excluding argument about missing witnesses. "[W]hen the witness is equally available to both sides, the preferred practice is to preclude the [missing witness] argument rather than to leave the jury free to speculate about a lot of non-evidence." *United States v. Simpson*, 974 F.2d 845, 848 (7th Cir. 1992). If Plaintff concludes that he has a basis to make out an exception to the rule pronounced in *Simpson*, he may raise his argument with the Court, but he must do so outside the presence of the jury and in advance of referencing any uncalled witnesses.

Defendants' argument regarding missing evidence is denied as overbroad. The Court could envision instances where the absence of evidence is relevant. For example, if Defendants fail to present any evidence, other than the testimony of the Defendants themselves, showing that Officer Bogdalek was not involved in Plaintiff's arrest, Plaintiff might reference that lack of evidence.

However, Defendants' motion to bar Plaintiff from arguing, directly or indirectly, that Defendants' spoliated evidence is granted for the reasons explained in response to Defendants' motion in limine #2.

Finally, Defendants' motion to exclude Officer Weber's dash cam video is granted in part and denied in part. The Court has not seen the video in question, and thus is unable to rule on its relevance generally. But to the extent that the video captures Officer Weber saying something to the effect of "Another fucking lawsuit!" after his interactions with Plaintiff, Defendants' motion is granted. That comment is irrelevant to the claims at issue in this lawsuit, and would open the door to additional irrelevant information regarding the Martinez family's history with the Chicago Police Department, which has the capacity of unfairly prejudicing both sides. See Fed. R. Evid. 401, 403. More importantly, this testimony would lead to an unnecessary sideshow that would distract the jury from the narrow set of relevant issues in this lawsuit.

### 27. Motion Missing

***17** There does not appear to be a motion #27, perhaps due to a numbering error.

### 28. Motion to Exclude Testimony of Liliana Ramos

Defendants move in limine to exclude the testimony of Plaintiff's girlfriend, Liliana Ramos, as irrelevant, as a waste of time, unfairly prejudicial, and improper character evidence. Defendants' motion is denied.

Plaintiff disclosed Ms. Ramos as a witness with knowledge of Plaintiff's damages. When deposed, Ms. Ramos confirmed that she has no first-hand knowledge of the events of January 17, 2012 (she was not present at the scene), and said that she intended to testify at trial as to "what kind of person [Plaintiff] is." [184-1, at 15.] In response to Defendants' motion, Plaintiff agrees that Mr. Ramos should be precluded from offering impermissible character evidence, but claims that her testimony is still relevant to explain how "this ordeal has impacted [Plaintiff's] life and his emotional and psychological distress." [196, at 2.] Plaintiff criticizes Defendants for failing to adequately inquire as to these issues during Ms. Ramos's deposition.

Having read Mr. Ramos's deposition transcript, the Court is skeptical as to the amount of admissible, non-cumulative testimony Ms. Ramos will have to offer. That being said, Plaintiff is entitled to present evidence relevant to his claim for damages, and as Plaintiff's girlfriend during and after the incident in question, Ms. Ramos has a sufficient foundation for testifying on this narrow issue. Suffice to say that, if Plaintiff chooses to call Ms. Ramos at trial, her testimony will be very brief, and Defendants of course are free to raise relevant objections to her testimony at trial.

### 29. Motion to Bar Certain Testimony of Sergeant Lance Becvar

Defendants move in limine to bar certain aspect of the testimony of Sergeant Lance Becvar. Ruling on Defendants' motion is reserved.

Sergeant Becvar is employed by the Chicago Police Department as a "supervisor in information services over the in-car camera systems." [185, at 1.] At his deposition, Sergeant Becvar testified about, *inter alia*, police officers' duty (pursuant to the Department's General Orders) to wear a lapel microphone, police officers' compliance rate for doing so, and Department strategy/initiatives for requiring officers to do so. Defendants seek to bar Sergeant Becvar from testifying as to these issues at trial, arguing that he is not an expert in this area and thus his testimony is unreliable and misleading. In response, Plaintiff says that he "does not object to the majority of this motion," [196, at 5], arguing that portions of Defendants' motion are overly broad and/or premature.

Breaking this argument down, as to Sergeant Becvar's testimony regarding the Chicago Police Department's general orders regarding lapel microphones, as stated above, the general rule is that "any attempt to use violations of CPD General Orders or other policies and procedures as prima facie evidence of a constitutional violation is prohibited," but there "may be other circumstances in which this kind of evidence is admissible." *Gonzalez*, 2015 WL 3671641, at *13. The admissibility of such evidence hinges primarily on (a) whether the evidence is relevant, and (b) the extent to which the evidence might prejudice the jury. And the Court also noted that while evidence relating to lapel microphones sits at the outskirts of the relevance spectrum, it may be at least relevant to Plaintiff's conspiracy claim (*e.g.*, whether Defendant Weber intended to hide his conspiratorial agreement with his co-Defendants), and thus the Court will reserve ruling

on this point until trial. To be sure, even if limited testimony is admitted on this issue, the Court has stressed that it will not permit a sideshow on ancillary evidentiary points such as this, and the prospect of calling a separate witness on this point after questioning Defendant Weber raises a yellow flag indicating that Plaintiff may be taking this issue too far. Thus, ruling is reserved. If the Court permits any testimony from Sgt. Becvar, it will entertain objections should Plaintiff's presentation of this evidence become irrelevant, cumulative, or prejudicial.[9] Fed. R. Evid. 401, 403. Plaintiff must also provide a foundation to show that Sergeant Becvar is competent to testify regarding the Department's requirements.

***18** Second, Plaintiff does not object to omitting Sergeant Becvar's testimony regarding officers' compliance rates for wearing lapel microphones, and thus Defendants' motion is granted as to this point.

Third, Plaintiff argues that Defendants' objection to Sergeant Becvar testifying about CPD strategy/initiatives regarding lapel microphones is overly broad and vague. Plaintiff says that the only testimony that falls into this category is a statement about officer discipline for failing to wear lapel microphones (*i.e.*, part of the Department's strategy for gaining compliance is to discipline those who do not properly use the A/V surveillance systems), and thus that any ruling on this part of Defendants' motion would not provide the parties with any meaningful limitation. The Court disagrees. CPD strategy and initiatives relating to their A/V surveillance systems is irrelevant to the issues in this trial. This part of Defendants' motion is granted.

### C. Plaintiff's Motions in Limine

#### 1. (A) Motion to Bar Use of Undisclosed Documents to Refresh Recollection

Plaintiff moves in limine to bar Defendant Bogdalek from using materials not produced during discovery to refresh her recollection. More specifically, Plaintiff says that Defendant Bogdalek has testified that she remembers very little about the day of Plaintiff's arrest, and Plaintiff is concerned that Ms. Bogdalek might appear at trial "with a suddenly reinvigorated memory" through her review of notes that she prepared for her attorneys at the time of the incident. It is unclear whether these documents actually exist, but apparently Defendants invoked the attorney–client privilege in response to Plaintiff's inquiries about any such documents. Plaintiff's motion is denied.

Although neither party cites it, Federal Rule of Evidence 612 governs this motion. The rule "gives an adverse party certain options when a witness uses a writing to refresh memory * * * before testifying, if the court decides that justice requires the party to have those options." Fed. R. Evid. 612(a), (a)(2). Ordinarily, the "adverse party is entitled to have the writing produced at the hearing, to inspect it, to cross-examine the witness about it, and to introduce in evidence any portion that relates to the witness's testimony." Fed. R. Evid. 612(b). However, the Notes of the House Judiciary Committee clarify that "nothing in the Rule [should] be construed as barring the assertion of a privilege with respect to writings used by a witness to refresh his memory." Fed. R. Evid. 612, Notes of Committee on the Judiciary, H. Rep. 93-650. To be sure, certain privileges are qualified, and thus can be overcome if the adverse party can demonstrate sufficient need for the documents, but no such arguments have been made here. See, *e.g.*, *E.E.O.C. v. Continental Airlines, Inc.*, 395 F. Supp. 2d 738, 744–45 (N.D. Ill. Oct. 11, 2005). In fact, it is still unclear whether these documents even exist, even though this issue arose prior to the close of discovery. But discovery has now been closed for more than 16 months, and the time for arguing about document production and privilege logs has long since passed.

#### 2. (B) Motion to Bar Evidence Unrelated to Probable Cause

***19** Plaintiff moves in limine to bar a series of potential topics as irrelevant pursuant to Federal Rule of Evidence 402, which says that "[i]rrelevant evidence is not admissible." Fed. R. Evid. 402. Specifically, Plaintiff alleges that the only basis for relevance is "whether the Defendants had probable cause to search, seize, arrest, and charge," and Plaintiff claims that certain evidence related to (1) the arrest of Alberto Martinez, (2) the use of mugshots, and (3) the school lockdown that took place during the officer's search for Alberto Martinez are all categorically irrelevant. Plaintiff's motion is denied.

First, the evidence relating to the arrest of Alberto Martinez is highly relevant and, contrary to Plaintiff's assertions, not unfairly prejudicial to Plaintiff. As

mentioned throughout these motions in limine, the scope of relevance in this case is narrow, and relates primarily to the events that occurred in the middle of the afternoon on January 17, 2012. And the sole reason that the officers encountered Plaintiff on that day is because of the actions of Plaintiff's brother, Alberto. Thus, the officers' accounts of the pursuit and arrest of Alberto Martinez, Alberto Martinez's conduct, and Alberto Martinez's relationship to Plaintiff, all inform the circumstances under which officers entered the home and conducted their search. To be sure, there are facts about Alberto Martinez that are irrelevant to this case, and there could be a point at which Defendants' presentation of facts about Alberto Martinez becomes cumulative, but Plaintiff has failed to articulate any set of facts that is categorically excludable at this point. Plaintiff's motion is denied, and Plaintiff may raise relevance objections at trial.

Second, Plaintiff moves to bar Defendants from introducing mug shot photos of Daniel and Alberto Martinez, which Plaintiff surmises Defendants will use to show the resemblance between the brothers. But this information is relevant to the legal claims in this case to the extent that any of the arresting officers contends that he or she thought that Plaintiff was the suspect in question. See, *e.g.*, *Common v. City of Chicago*, 661 F.3d 940, 943 (7th Cir. 2011) (the objective reasonableness of an officer's actions is based in part on the "circumstances known and the information available to the officer at the time of his action"). In reply, Plaintiff withdrew his objection to the use of Plaintiff's mugshot (assuming it is "scrubbed" of police data and not referred to as a "mug shot," which the Court agrees is appropriate to avoid Fed. R. Evid. 403 concerns), but maintains that Alberto Martinez's mug shot is irrelevant. The Court disagrees— the extent to which the brothers may resemble each other is relevant. This motion is denied.

Third, Plaintiff seeks to exclude evidence that a local school was on lockdown while the police searched for Alberto Martinez. Defendants argue that this fact is relevant to the determination of probable cause, which considers "the facts as they reasonably appeared to the arresting officer, seeing what he saw, hearing what he heard, and so forth." *Holmes v. Vill. of Hoffman Estates*, 511 F.3d 673, 679 (7th Cir. 2007). The Court agrees. The nature and exigency of the search in question is directly relevant to the reasonableness of the officers' actions in conducting the search. Although a gratuitous presentation of this fact could exceed the bounds of relevance (Fed. R. Evid. 401, 403), the fact itself is not categorically excludible. This motion is denied.

### 3. (C) Motion to Bar Evidence of Fifth Amendment Privilege

***20** Plaintiff moves in limine to exclude evidence that Plaintiff and Alberto Martinez previously asserted the Fifth Amendment privilege during depositions in this case.

Defendants do not object to the exclusion of evidence regarding Plaintiff's invocation of the Fifth Amendment, "unless Plaintiff opens the door." [147, at 13.] This part of Plaintiff's motion is granted. To the extent Defendants believe that Plaintiff has opened the door on this issue, they should inform the Court at a sidebar outside of the presence of the jury before raising the issue.

But Defendants vigorously object to this motion as it relates to Alberto Martinez, arguing that his Fifth Amendment invocation is relevant and probative. However, as noted above, all parties have agreed that Alberto Martinez will not be called to testify at trial. Accordingly, this motion is denied as moot insofar as it applies to Alberto Martinez.

### 4. (D) Motion to Bar Argument that Oral Statements Amount to Probable Cause

Plaintiff moves in limine to bar Defendants from arguing that Plaintiff's verbal resistance constituted probable cause to arrest Plaintiff for obstructing the arresting officer's access to a room. Plaintiff's motion is denied.

Plaintiff has failed to articulate an evidentiary concern that is appropriate for pre-trial resolution. Plaintiff's argument, it seems, is that Defendants did not have probable cause to arrest Plaintiff. The parties are free to argue this point at trial based on the evidence presented during trial, and the Court will instruct the jury as to the applicable law. If Plaintiff is concerned that Defendants are, "at the eleventh hour, * * * manufactur[ing] new theories of probable cause" [154, at 12], they are free to impeach the officers with their pre-eleventh-hour theories. And both parties are free to object at trial should either party misstate the law to the jury.

### 5. (E) Motion to Bar Evidence About Pulling Away to Defeat Arrest

Plaintiff moves in limine to bar Defendants and their witnesses from speculating that Plaintiff pulled away to "defeat his arrest." [141, at 8.] Plaintiff agrees that the arresting officer(s) can testify that Plaintiff pulled away from them, but he seeks to bar the officer(s) from concluding that Plaintiff did so "to defeat arrest." While in theory this seems like a speculative comment, the Court concludes that there are too many variants of this response that hover the line of admissibility to warrant pre-trial guidance from the Court. For example, if an officer testified that Plaintiff pulled away to such an extent that he precluded the officer from executing the arrest, that would be essentially the same response absent any speculation. With the admonition that the arresting officers likely would not be competent to testify as to *why* Plaintiff moved his body in a particular manner, Plaintiff's motion is denied, and Plaintiff is free to raise speculation-based objections at trial.

### 6. (F) Motion to Bar Evidence or Argument About Attorneys

Plaintiff moves in limine to bar evidence or argument about the fact that Jared Kosoglad represented Plaintiff or any other person in any other proceeding. Plaintiff's motion is granted.

***21** Defendants point multiple examples of how Ms. Kosoglad has injected himself into the storied civil and criminal history of the Martinez family, but the Court has done its best in this rulings to make clear that this history is irrelevant to the narrow issues being tried here. Because the Court is barring Plaintiff from raising these subjects, so too Defendants are prohibited from side-tracking this trial by questioning the ethics of Mr. Kosoglad.

### 7. (G) Motion to Bar Misstating Fourth Amendment Law

Plaintiff moves in limine to bar Defendants from arguing that probable cause to enter one unit in a multi-unit building provides probable cause to search the entire building. Plaintiff's motion is denied. It is the duty of the Court, not the parties, to instruct the jury on the law. Here, the law is fact dependent, and thus it is not apparent that either party's theory on the reasonableness of the officers' search violated the Fourth Amendment. See, *e.g.*, *United States v. Butler*, 71 F.3d 243, 249 (7th Cir. 1995) ("[W]hen a building is divided into more than one residential unit, a distinct probable cause determination must be made for each unit. * * * There is an exception * * *, however, where 'although appearing to be a building of several apartments, the entire building is actually being used as a single unit.' When this is the case, a finding of probable cause as to a portion of the premises is sufficient to support a search of the entire structure.") (internal citations omitted). The Court will work with the parties in fashioning an appropriate jury instruction on the law and will entertain objections regarding misrepresentations of the law to the jury.

### 8. (H) Motion to Bar Improper Bolstering of Defendants' Character

Plaintiff moves in limine to bar Defendants from introducing evidence seeking to bolster the character of Defendants,[10] such as with testimony about accommodations or awards. Defendants agree to refrain from introducing such evidence, unless Plaintiff first attacks the credibility of these witnesses. Plaintiff's motion is granted.

### 9. (I) Motion to Bar Evidence Regarding Drug or Alcohol Use

Plaintiff moves in limine to bar evidence, argument, or implication regarding Plaintiff's use of illegal drugs or alcohol. Defendants agree to refrain from making any such arguments unless Plaintiff opens the door. Plaintiff's motion is granted. To the extent Defendants believe that Plaintiff has opened the door to such arguments, they should raise the issue with the Court outside of the presence of the jury before making their arguments.

### 10. (J) Motion to Bar Evidence Regarding Attorneys' Fees

Plaintiff moves in limine to bar any reference to Plaintiff's fee arrangement with his attorneys. Defendants agree,

except they contend that the jury instruction on damages should mention that the jury need not consider attorney fees in determining damages. Plaintiff disagrees with Defendants' jury instruction comment. Plaintiff's motion is granted, and the Court will resolve the jury instruction issue in due course.

### 11. (K) Motion to Exclude Non-Party Witnesses from the Courtroom

***22** Plaintiff's unopposed motion to exclude non-party witnesses from the courtroom is granted.

### 12. (L) Motion to Bar Argument Regarding Excessive Damages

Plaintiff moves in limine to bar Defendants from arguing during closing that (1) Plaintiff has asked for more money than he expects to be awarded, (2) Plaintiff's recovery is not subject to income tax, (3) defense counsel is shocked by Plaintiff's damages request, and (4) the damages request, or Plaintiff's case, would place a burden upon the public as a whole, or increase taxes, or increase the budget deficit for the City which is suffering from financial difficulties. Defendants do not object to Plaintiff's motion as written, but reserve their right to argue that the damages sought are excessive, disproportionate to the damages actually incurred, or entirely inappropriate. Plaintiff agrees to this carve out. Thus, Plaintiff's motion is granted.

### 13. (M) Motion to Bar Evidence of Prior Arrests and Convictions

Plaintiff moves in limine to bar reference to any and all of Plaintiff's prior arrests and convictions, if any, except as may be relevant to Plaintiff's claim of retaliation. Defendants agree, "so long as Plaintiff does not attempt to testify that he has never been arrested before or the like." [147, at 24.] Plaintiff did not object to this response. Thus, Plaintiff's motion is granted.

### 14. (N) Motion to Bar Characterization of Area as "High Crime"

Plaintiff moves in limine to bar reference to the arrest location as a "high crime" area. Defendants agree to this motion. Plaintiff's motion is granted.

### 15. (O) Intentionally Omitted

Plaintiff's motion in limine "O" is intentionally omitted.

### 16. (P) Motion to Bar IPRA Records

Plaintiff moves in limine to bar evidence relating to the City of Chicago's IPRA records from the January 17, 2012 incident. Defendants agree, and thus the motion is granted.

### 17. (Q) Motion to Bar Background Investigations of Jurors

Plaintiff moves in limine to bar Defendants to gain an "unfair advantage" by accessing certain databases to investigate the background of jurors, including CLEAR (Citizen Law Enforcement and Reporting) and LEADS (Law Enforcement Agencies Data System). Plaintiff's motion is granted.

"The propriety of allowing a litigant in a civil case to access police databases to perform background checks on potential jurors and to use such information during *voir dire* is an unsettled question in this district." *Dyson v. Szarzynski*, 2014 WL 7205591, at *2 (N.D. Ill. Dec. 18, 2014). The Court is sensitive to the potential pitfalls of allowing background checks (*e.g.*, empowering jurors to conduct their own background checks of the parties, creating an imbalance of information among the parties), as well as the potential benefits (*e.g.*, the importance of a rigorous and candid *voir dire* process), as discussed in great detail in the *Dyson* opinion. *Id.* at *2–4. But the logistical hurdles to accomplishing this background search combined with the potential imbalance of information (*i.e.*, even if background checks are made available to both parties, this only backstops one aspect of juror impartiality; namely, one aspect of greater importance to Defendants derived from Defendants' proprietary search software) persuade the Court that exclusion of background checks is the appropriate course of action for this trial. See also *Gonzalez v. Olson*, 2015 WL 3671641,

at *8 (N.D. Ill. June 12, 2015) ("Defendants' asserted justification that jurors will lie about their criminal history or arrest record is not such a pervasive problem that it needs to be addressed by conducting criminal background checks on all jurors.").

**18. (R) Motion to Bar Testimony Regarding 2624 W. 55th Street**

***23** Plaintiff moves in limine to bar undisclosed witnesses from testifying that they entered 2624 W. 55th Street prior to Plaintiff's arrest. Plaintiff's motion is denied.

As a general rule, neither party is entitled to present undisclosed witnesses at trial, and Defendants do not object to Plaintiff's motion in this regard. But properly disclosed witnesses may testify that they entered 2624 W. 55th Street prior to Plaintiff's arrest, and to the extent that Plaintiff disagrees with these witnesses, he may attempt to impeach them.

**19. (S) Motion to Bar Speculation by Erin Hanson**

Plaintiff moves in limine to bar speculation by Erin Hanson. Plaintiff does not explain who Erin Hanson is, or what speculative testimony she will offer. Plaintiff's motion is denied, and Plaintiff may object at trial should he feel that Ms. Hanson is speculating in violation of the Federal Rules of Evidence.

**20. (T) Motion to Include Adverse Inference Regarding Phone Records**

Plaintiff moves in limine to request that the Court instruct the jury that they should draw an adverse inference from Defendants Chavez and Weber's failure to produce their phone records. Plaintiff's motion is denied.

Plaintiff concedes that although he moved to compel the phone records in question, Magistrate Judge Cole denied that motion. [66.] Defendants nonetheless agreed to produce the phone records, and to some extent have done so (although they produced a spreadsheet containing edited information found on the actual phone records). While Defendants' production may be unsatisfactory, discovery in this case has been closed for more than 16 months, and the time to object to document productions has long since passed. In addition, in order to warrant an adverse inference instruction, Plaintiff must show that Defendants destroyed the documents in question in bad faith. *Park v. City of Chicago*, 297 F.3d 606, 615 (7th Cir. 2002) (adverse inference requires destruction of evidence in bad faith). But the only allegation here is that Defendants have withheld information, not that they destroyed it or that they did so in bad faith.

**21. (U) Motion to Include Adverse Inference Regarding Missing Videos**

Plaintiff moves in limine to request that the Court instruct the jury that they should draw an adverse inference from Defendants' failure to produce the videos from the cameras in Defendant Chavez and Weber's squad cars. Plaintiff's motion is denied.

As touched upon in the previous motion in limine, in order to be eligible for an adverse inference instruction, Plaintiff must demonstrate that (a) the documents contained adverse information, and (b) that Defendants "intentionally destroyed the documents in bad faith." *Norman-Nunnery v. Madison Area Tech. College*, 625 F.3d 422, 428 (7th Cir. 2010); see also *Everett v. Cook County*, 655 F.3d 723, 727 (7th Cir. 2011); *S.C. Johnson & Son, Inc. v. Louisville & Nashville R.R. Co.*, 695 F.2d 253, 258–59 (7th Cir. 1983) (same). As to the "adverse information" requirement, a violation of a records retention policy creates a rebuttable presumption that the missing evidence was unfavorable to the responsible party, but this does not eliminate the need to show bad faith in order to warrant the adverse inference instruction. See *Park v. City of Chicago*, 297 F.3d 606, 615 (7th Cir. 2002) (while the violation of a record retention regulation " 'creates a presumption that the missing record[s] contained evidence adverse to the violator,' " "absent bad faith, a violation of * * * [a] record retention regulation[ ] [does] not automatically trigger an adverse inference.") (quoting *Latimore v. Citibank Fed. Sav. Bank*, 151 F.3d 712, 716 (7th Cir. 1998)); *Beniushis v. Apfel*, 2001 WL 303548, at *4 (N.D. Ill. Mar. 27, 2001) ("[T]o impose the sanction of an evidentiary presumption adverse to the responsible party, it must be found both that (a) the missing evidence was likely unfavorable to the responsible party (which is the presumption drawn from violation of the regulation) and (b) the loss of the records was willful or in bad faith.");

*Richardson v. City of Chicago*, 2012 WL 3643908, at *6 (N.D. Ill. Aug. 22, 2012) (a district court need not address whether a document retention policy was violated if the movant fails to establish bad faith or intent).

***24** First, Plaintiff has failed to establish that the missing videos contained "adverse information." As explained in response to Defendants' motion in limine #2, Defendants' interactions with Plaintiff, including the arrest, took place indoors, and thus would not have been captured by the squad car cameras. At most, the video cameras would depict the officers moving about and/or conversing before and after Plaintiff's arrest, but absent any audio feed (which, as explained above, would have captured relevant information), the visual depiction of the officers alone is unlikely to be of any relevance. Plaintiff himself sat in a squad car after his arrest and thus had a vantage point similar to what the officer's surveillance camera would have seen, and yet Plaintiff has been unable to articulate any relevant evidence that might have been captured on the video surveillance systems.

Plaintiff argues that the "adverse information" requirement is presumed here because Defendants violated the Local Records Act, 50 ILCS 205 *et seq.*, and the Chicago Police Department's document retention policies. See *Latimore*, 151 F.3d at 716 ("The violation of a record retention regulation creates a presumption that the missing record contained evidence adverse to the violator."). In response, Defendants argue that it was *other* officers, not Defendants, who uploaded the mislabeled videos, and Plaintiff does not provide any argument or authority as to why the actions of these non-Defendant officers should be imputed to Defendants. More to the point, though, Defendants cite the 2015 Amendment to Fed. R. Civ. P. 37, which rejects giving adverse inference instructions where the offending party was negligent or even grossly negligent, commenting that "[i]nformation lost through negligence may have been favorable to either party, including the party that lost it, and inferring that it was unfavorable to that party may tip the balance at trial in ways the lost information never would have." Fed. R. Civ. P. 37(e)(2) Advisory Committee Note, 2015 Amendment. The Committee Note says that the Rule amendment rejects cases that authorize the giving of adverse-inference instructions on a finding of negligence or gross negligence, although the Committee is silent on how the amendment impacts presumptions based on document retention policies. The Committee did note, however, that "court[s] should be sensitive * * * to the fact that * * * independent preservation requirements may be addressed to a wide variety of concerns unrelated to the current litigation," and "[t]he fact that a party had an independent obligation to preserve information does not necessarily mean that it had such a duty with respect to the litigation." *Id.* The Seventh Circuit has not yet addressed how, if at all, the Rule 37 amendment impacts its rulings on adverse inferences. But the Court need not resolve that issue here because Plaintiff has failed to meet his evidentiary burden of demonstrating that Defendants destroyed the videos in bad faith.

As Plaintiff notes, the Chicago Police Department retains all surveillance footage for 90 days unless the footage relates to a felony arrest or labeled as having evidentiary value to law enforcement or for a legal proceeding, in which case it is preserved indefinitely. Video footage is labeled and uploaded by the on-site officers through a pop-up menu in their squad cars. Although Alberto Martinez was arrested for a felony, non-Defendant officers from Beats 911 and 913 mislabeled the two video recordings in question as a "traffic stop" and a "training video" respectively, meaning that they were not flagged for preservation and thus were automatically purged after 90 days. However, there is no evidence that these non-Defendant officers acted in bad faith in mislabeling these videos, or that the alleged mistakes of the non-Defendant officers should somehow be imputed to Defendants. The only colorable evidence of bad faith offered by Plaintiff relates to Defendant Weber's comment, "Oh great, another lawsuit," which he allegedly said after Plaintiff's arrest. Although not enough to demonstrate bad faith on its own, this comment shows that Defendant Weber was aware of the potential for litigation (or that he was "sensitive to the possibility of suit," as Plaintiff says), and therefore that he had a responsibility to preserve the video footage (to the extent the video had evidentiary value, which the Court finds unlikely). Regardless, the surveillance footage from Defendant Weber's squad car *was* preserved (it was uploaded and labeled as relating to a felony arrest by his partner, Officer Buehler), and that video was produced to Plaintiff. Plaintiff's failure to establish bad faith is fatal to his motion. Plaintiff has not provided any evidence indicating that either Defendant Chavez or Defendant Bogdalek acted in bad faith with regard to the non-Defendant officers' mislabeling of the surveillance videos, despite his burden to do so.

Accordingly, Plaintiff's motion for an adverse inference is denied. [11]

### 22. (V) Motion to Bar Arguments Regarding the Risks of Police Work

***25** Plaintiff moves in limine to bar Defendants from arguing that "police officers risk their lives every day," or other similar comments about the general risks involved with police work. Plaintiff's motion is denied. Both parties have leeway in making their closing arguments, and Defendants' invocation of the general risks of police work is not so far beyond the scope of relevance or so prejudicial that it requires exclusion under Rules 401 or 403. However, the Court will entertain objections at trial should Defendants' arguments become gratuitous or otherwise violate the Federal Rules of Evidence.

## III. Conclusion

For the foregoing reasons, Defendants' motion for partial summary judgment [174] is granted. Defendants' motions in limine 1–29 [140, 184, 185] and Plaintiff's motions in limine A–V [141], are granted in part and denied in part. As a housekeeping matter, Defendants' motion to file instanter an amended reply in support of Defendants' motion in limine no. 2 [163] is granted. This case remains set for a further pretrial conference on July 6, 2016 at 1:15 p.m.

### All Citations

Not Reported in F.Supp.3d, 2016 WL 3538823

Footnotes

1 The parties allude to the fact that the "home" in question was actually two homes that somehow were connected to each other. The home that the suspect, Alberto Martinez, entered was 2622 West 55th Street, and Plaintiff Daniel Martinez lived at 2624 West 55th Street. When Officer Weber encountered Plaintiff, Plaintiff was in his residence, not the residence that Alberto Martinez entered. It is unclear how Officer Weber, or any other officer, accessed the 2624 West 55th Street property. [198, ¶¶ 1–2.]

2 "A person who knowingly resists or obstructs the performance by one known to the person to be a peace officer * * * of any authorized act within his or her official capacity commits a Class A misdemeanor." 720 ILCS 5/31-1(a).

3 The concern is that a jury might mistake evidence that an officer violated a policing standard as evidence that the officer also violated the Constitution. In certain instances, this concern can be addressed by instructing the jury as to the permissible uses of the evidence in question.

4 The extent of allowable questioning of Officer Bogdalek will be determined on a sliding scale based on Plaintiff's ability to lay a foundation regarding her role in Plaintiff's arrest. For example, if Plaintiff's counsel were to present Officer Bogdalek as his first witness, the Court would significantly limit the scope of Plaintiff's examination. However, if Plaintiff presents multiple witnesses who testify that Officer Bogdalek did in fact play a significant role in Plaintiff's arrest, the Court likely will expand the scope of permissible testimony.

5 Defendants acknowledge that Ms. Martinez did not consent to the officers' entry into the home, and instead argue that they were permitted to enter the home under exigent circumstances.

6 Seventh Circuit Pattern Jury Instruction § 7.24 (emphasis added).

7 See Fed. R. Evid. 801(d)(2)(E); *United States v. Pust*, 798 F.3d 597, 602 (7th Cir. 2015) ("For a co-conspirator's statements to be admissible under FRE 801(d)(2)(E), the government must establish by a preponderance of the evidence (1) that a conspiracy existed, (2) that the defendant and the declarant were members of the conspiracy, and (3) that the statements were made in furtherance of the conspiracy.").

8 At the first pretrial conference, counsel for Plaintiff stated that Plaintiff will not be calling Ms. McClellan as a witness and counsel for all parties confirmed that nobody will call Plaintiff's brother, Alberto Martinez.

9 Plaintiff agrees that Sergeant Becvar lacks knowledge to testify about the history of the Department's general orders regarding the use of lapel microphones or A/V surveillance generally.

10 As mentioned above, " '[b]olstering' is the practice of offering evidence solely for the purpose of enhancing a witness's credibility before that credibility is attacked. Such evidence is inadmissible because it 'has the potential for extending the length of trials enormously, * * * asks the jury to take the witness's testimony on faith, * * * and may * * * reduce the care with which jurors listen for inconsistencies and other signs of falsehood or inaccuracy." *Lindemann*, 85 F.3d at

1242 (quoting *LeFevour*, 798 F.2d at 983). But once a witness's credibility has been attacked, "the non-attacking party is permitted to admit evidence to 'rehabilitate' the witness." *Id.*

11 The Court is persuaded by the Advisory Committee's comment that the remedies in Fed. R. Civ. P. 37(e)(2) are "severe measures" and "should not be used when the information lost was relatively unimportant or lesser measures such as those specified in subdivision (e)(1) would be sufficient to redress the loss." Fed. R. Civ. P. 37(e)(2) Advisory Committee Note, 2015 Amendment. The Committee emphasizes that an adverse inference instruction is not the only available remedy under Rule 37(e)(2), and that "subdivision (e)(2) would not prohibit a court from allowing the parties to present evidence to the jury concerning the loss and likely relevance of information and instructing the jury that it may consider that evidence, along with all the other evidence in the case, in making its decision," instead of "instructing a jury it may draw an adverse inference from loss of information." *Id.* Here, Plaintiff has only moved in limine for an adverse inference instruction, and so the Court has no occasion to determine whether a less severe remedy might be available.

**End of Document**

2017 WL 4173358
Only the Westlaw citation is currently available.
United States District Court,
W.D. New York.

Wakeesha N. MOODY, Plaintiff,
v.
CSX TRANSPORTATION, INC., New York Central Lines, LLC and NYC Newco, Inc., Defendants.

07–CV–6398P
|
Signed 09/21/2017

**Attorneys and Law Firms**

Michael A. Bottar, Bottar Leone, PLLC, Syracuse, NY, for Plaintiff.

Jonathan P. Harmon, McGuire Woods LLP, Richmond, VA, Susan C. Roney, Nixon Peabody LLP, Laurie Styka Bloom, Nixon Peabody LLP, Buffalo, NY, for Defendant.

MARIAN W. PAYSON, United States Magistrate Judge

DECISION & ORDER

**PRELIMINARY STATEMENT**

***1** Plaintiff Wakeesha N. Moody ("Moody") has sued defendants CSX Transportation, Inc. ("CSX"), New York Central Lines, LLC, and NYC Newco, Inc., (collectively, "defendants") for personal injuries sustained in a railway accident. (Docket # 1–2). On June 16, 2006, Moody attempted to crawl underneath a train car located in a railyard operated by CSX in Lyons, New York (the "Lyons yard"). The train car began moving while Moody was beneath it, and she was dragged approximately twenty feet, resulting in injuries including an above-the-knee amputation of her left leg and the loss of toes on and crush injuries to her right leg. Following the Court's entry of a Decision and Order granting in part and denying in part defendants' motion for summary judgment (Docket # 90), the only claims that remain are for failure to warn by sounding a horn or bell prior to moving the train car and for failure to post appropriate warning signage in the Lyons yard.

Currently pending before this Court are three motions. (Docket ## 65, 68, 98). First, defendants have moved to exclude testimony from Moody's expert Stephen Timko ("Timko") on the grounds that Timko's proffered opinions are not appropriate subjects for expert testimony and do not meet the standards for admissibility established by *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993). (Docket # 65). Second, Moody has moved for spoliation sanctions. (Docket # 68).[1] Finally, defendants have moved to bifurcate the trial and try the issue of liability first and proceed only to the issue of damages in the event the jury determines that defendants are liable. (Docket # 98). Oral argument on the three pending motions was held on August 2, 2017. (Docket # 105).

## I. Defendants' Motion to Exclude Testimony from Timko

### A. Factual Background

Moody has disclosed Timko as an expert witness who is expected to testify at trial. (Docket # 65–2). Timko has 49 years of experience in the railroad industry, and for the last 16 years has owned a railroad consulting service. (*Id.* at 5). His prior experience includes serving as the Vice President and General Manager of Western New York & Pennsylvania RR, LLC, Assistant Superintendent for Train Operations for the Norfolk Southern Railroad, and Manager of Operations Planning for Conrail. (*Id.* at 6). According to Timko's expert report, his opinions are based on his knowledge, experience, and training, as well as his review of the following information: the deposition transcripts of Moody, witness Tiffany Johnson, CSX conductor Richard Roden, CSX engineer Frederick Albrecht, CSX police officer Gary Gawronski, and CSX police officer Alan Lee; CSX's responses to plaintiff's notices to produce and interrogatories; the Lyons Police Department accident report; the statements of Sheldon Davis, Tiffany Johnson, Joseph Monk, Richard Roden, and Frederick Albrecht; the tax map of the Lyons yard; photographs of the Lyons yard; a diagram of the Lyons yard; a video of the Lyons yard and surrounding area taken in 2008; and, his field inspection of the Lyons yard made from public property on January 17, 2015. (*Id.* at 9–10). Timko's expert report includes the following opinions: CSX failed to properly inform, educate, observe, and enforce a ban on pedestrian traffic at the Lyons yard; CSX failed to enlist the assistance of both the Lyons Police Department and the Wayne County Sheriff's Office

to prevent pedestrian traffic at the Lyons yard; CSX failed to educate local political officials, media personnel, law enforcement personnel, local residents, and its own employees by sponsoring Operation Lifesaver events in Lyons;[2] CSX failed to erect fences or barricades to prohibit the movement of the public onto the rail lines and railroad property in Lyons; CSX failed to properly post the Lyons yard with signs indicating potential dangers to the public; CSX failed to acknowledge observations by their own agents and other employees that the Lyons yard was used as a "private sidewalk for local residents"; CSX failed to properly train its agents and officers in order to protect the integrity of evidence in the event of an accident, specifically locomotive video equipment, downloadable event recorder information, and audio recordings; CSX failed to properly dispatch personnel, gather and protect evidence, and document the accident scene; and, CSX failed to ensure that its operating personnel, including train and engine service crews, comply with the operating rules, safety rules, and other issued special instructions, notices, and bulletins. (*Id.* at 10–11).

***2** As noted above, in light of the Court's decision on defendants' motion for summary judgment, the only claims that remain in this matter are for failure to warn by sounding a horn or bell prior to moving the train car and for failure to post appropriate warning signage in the Lyons yard. (Docket # 90 at 26–27). Moody's counsel acknowledged at oral argument that Timko's opinions unrelated to these two claims are no longer relevant. Accordingly, the Court has limited its recitation of the facts to those relevant to the remaining claims.

Timko was deposed on November 17, 2015. (Docket # 65–3). Timko testified that in order to prepare his report, he spent several hours reviewing materials related to this case, including photographs, police reports, maps, and statements regarding the accident scene, and that he performed an inspection at the Lyons yard on January 17, 2015. (*Id.* at 83–87). According to Timko, his inspection of the Lyons yard occurred from public property, and he did not enter railroad property at any time. (*Id.* at 85–86).

Timko testified that CSX had a "lackadaisical attitude toward public safety" at the Lyons yard and that despite having received numerous reports of pedestrians in the yard (prompting the CSX Police Department to refer to the Lyons yard as a "public sidewalk"), CSX took no action to address the issue. (*Id.* at 106). According to Timko, when he visited the Lyons yard, he observed footprints in the snow and individuals walking through the yard, with nobody policing the station. (*Id.* at 106–07). He testified that he saw an adult man walk across the track. (*Id.* at 107–08).

Timko objected to the characterization of pedestrians in the Lyons yard as "trespassers," explaining that "you can't be a trespasser unless it's posted." (*Id.* at 126). Because there were no "No Trespassing" signs posted at the Lyons yard, Timko opined that pedestrians had no way of knowing they were not permitted to cross, and Moody was therefore not trespassing at the time of her accident. (*Id.* at 127–28). Timko later acknowledged, however, that he did not know whether there were "No Trespassing" signs posted and stated that his opinion would be the same whether there were "some or none or lots" of such signs. (*Id.* at 130–31). Timko stated that it was necessary, in addition to posting signs, to educate people about the dangers because it is impossible to fence in the entire right-of-way. (*Id.* at 131–32). Timko further testified that CSX could have posted signs in the Lyons yard stating, "No Access," "Use Bridge," "Use Route 14 Bridge," "Private Property," "Dangerous," "High Speed Trains," or similar warnings. (*Id.* at 155–56). Timko continued that CSX could have posted a sign saying "Dangerous area, Do not enter tracks" or "any kind of signage you want to put up there." (*Id.* at 157). Timko elaborated that the warning signs "could have said something like, 'dangerous, high-speed traffic area—high speed trains' " and that CSX "needed to do some education." (*Id.* at 159). Timko also opined that, in his experience, it was standard practice in the railroad industry to put up signs posting private property. (*Id.* at 142–43).

Timko also submitted an affidavit dated April 1, 2016, in opposition to defendants' motion. (Docket # 69–5). In his affidavit, Timko alleges that the answers he gave at his deposition do not represent his full and complete opinions. (*Id.* at ¶ 2). Timko states that on June 15–16, 2006, good and accepted standards of practice required defendants to sound the train horn and bell just prior to moving the train and that defendants' failure to do so was a deviation from such good and accepted standards of practice. (*Id.* at ¶¶ 3, 5). Timko further states that CSX is a full member of the Northeast Operating Rules Advisory Committee ("NORAC") and attaches for the Court's review a copy of the NORAC operating rules that were in place on June 15–16, 2006. (*Id.* at ¶¶ 6–7,

Ex. A). Timko explains that NORAC operating rules 19 and 20 required the locomotive engine bell and horn to be sounded before train movement and that defendants' internal rules imposed a similar requirement. (*Id.* at ¶¶ 9–10). Timko also opines that good and accepted standards of practice required defendants to post signs in and around the Lyons yard stating, *e.g.*, "No Trespassing," "Private Property," and "Danger," in order "to serve as a warning to pedestrians about dangers in the Yard that they may not appreciate." (*Id.* at ¶ 16).

**B. The Parties' Positions**

***3** Defendants ask the Court to exclude Timko's opinions and testimony in their entirety. (Docket # 65–4 at 1–2). Defendants contend that Timko's opinions, by his own admissions, are based on "nothing more than his review of litigation documents, an internet search and observations he was able to make while seated briefly in his car parked off railroad property on a cold winter day some nine years after the incident." (Docket # 65–4 at 2). Defendants further argue that: (1) the subject matters on which Timko seeks to opine are matters that the jury can discern without the need for expert testimony; (2) Timko's opinions are based on an incomplete and/or incorrect understanding of the evidence; (3) Timko has applied no reliable methodology but has instead relied upon speculation; and, (4) none of Timko's opinions are supported by scientific or technical evidence. (*Id.* at 3).

As a threshold matter, defendants maintain that Timko's proffered opinions are not proper subjects of expert testimony. (*Id.* at 6). Defendants argue that "[t]he role of an expert is to fill specific gaps in the jury's knowledge about technical matters that are outside the ken of the average juror" and that "[a] jury is perfectly competent to determine whether warnings were given, whether a fence was erected, whether [CSX] trained its personnel, and whether [CSX] acknowledged observations about the nature of the short-cut [Moody] used." (*Id.* at 6–7). Defendants further argue that Timko's testimony would serve only to "bolster [Moody's] claim by attaching an 'expert' label to it." (*Id.* at 7).

Defendants also argue that Timko's proffered opinions do not satisfy the *Daubert* standard for admissibility. (*Id.* at 9). According to defendants, "there is no scientific theory, let alone one that has been tested with reliable certainty, that supports Timko's proposed testimony." (*Id.* at 11). Defendants further contend that Timko has offered only conclusory observations and that his opinions are not supported by "any recognized theory or methodology." (*Id.*).

With respect to Timko's opinions regarding CSX's alleged failure to warn, defendants argue that they should be excluded because (1) Timko improperly opines on legal conclusions, and (2) Timko's opinions lack an evidentiary basis and are based solely on speculation and *ipse dixit*. (Docket ## 65–4 at 13–14; 76 at 7–12).

Moody counters that Timko's testimony is admissible under *Daubert* because Timko is qualified as an expert and his testimony is reliable and will assist the trier of fact. (Docket # 70 at 5–10). Specifically, Moody argues that Timko has "specialized knowledge," gained from his extensive experience in the railroad industry, that will help inform the jury regarding the relevant industry standard for railroads. (*Id.* at 7–9). With respect to Timko's opinions regarding CSX's alleged failure to sound a bell or horn, Moody maintains that they are based upon the testimony of Moody and witness Tiffany Johnson, and that defendants' arguments regarding Timko's factual assumptions go to the weight of the testimony, not its admissibility. (*Id.* at 11). Additionally, Moody argues that testimony as to legal conclusions is not inadmissible *per se* and that Timko's opinions fall within the ambit of his training and experience. (*Id.* at 10–11). With respect to Timko's opinions regarding the failure to post signs, Moody argues that defendants have mischaracterized his testimony and that he should be permitted to opine that accepted standards of care required defendants to post warning signs. (*Id.* at 12–13).

**C. Analysis**

Rule 702 of the Federal Rules of Evidence requires that a proposed expert witness be qualified on the basis of "scientific, technical, or other specialized knowledge [that] will help the trier of fact to understand the evidence or to determine a fact in issue." Fed. R. Evid. 702. Accordingly, an expert may provide testimony if (1) "the testimony is based upon sufficient facts or data"; (2) "the testimony is the product of reliable principles and methods"; and, (3) "the expert has reliably applied the principles and methods to the facts of the case." *Id.* The trial court must fulfill a "gatekeeping" duty under Rule 702 to ensure that any expert testimony to be admitted is "not only relevant, but reliable." *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. at 589, 113 S.Ct. 2786; *see also Kumho Tire Co.,*

*Ltd. v. Carmichael*, 526 U.S. 137, 147, 119 S.Ct. 1167, 143 L.Ed.2d 238 (1999). Thus, the trial court's inquiries should focus on three issues: "(1) whether the witness is qualified to be an expert; (2) whether the opinion is based upon reliable data and methodology; and (3) whether the expert's testimony on a particular issue will assist the trier of fact." *Arista Records LLC v. Lime Grp. LLC*, 2011 WL 1674796, *1 (S.D.N.Y. 2011) (citing *Nimely v. City of New York*, 414 F.3d 381, 396–97 (2d Cir. 2005)).

***4** Under *Daubert* and *Kumho Tire*, a court must "first determine whether the proffered expert testimony is relevant." *Am. Ref–Fuel Co. of Niagara, LP v. Gensimore Trucking, Inc.*, 2008 WL 1995120, *3 (W.D.N.Y. 2008). Further, the testimony must "help the trier of fact to understand the evidence or to determine a fact in issue." Fed. R. Evid. 702; *see also Daubert*, 509 U.S. at 591, 113 S.Ct. 2786; *Campbell v. Metro. Prop. & Cas. Ins. Co.*, 239 F.3d 179, 184 (2d Cir. 2001). The question is one of "fit," meaning that the evidence must be "sufficiently tied to the facts of the case." *Daubert*, 509 U.S. at 591, 113 S.Ct. 2786 (quoting *United States v. Downing*, 753 F.2d 1224, 1242 (3d Cir. 1985)). Where an expert opinion is based upon assumptions that are not present in the case, the opinion "cannot be said to 'assist the trier of fact' as Rule 702 requires." *Elcock v. Kmart Corp.*, 233 F.3d 734, 756 n.13 (3d Cir. 2000). Thus, such an opinion "misleads the fact-finder and arguably does not comply with the 'fit' requirement of that Rule." *Id.*

After determining that the proffered testimony is relevant, the court must determine whether the proffered testimony "has a sufficiently 'reliable foundation' to permit it to be considered." *Am. Ref–Fuel Co. of Niagara, LP v. Gensimore Trucking, Inc.*, 2008 WL 1995120 at *3 (quoting *Campbell v. Metro. Prop. & Cas. Ins. Co.*, 239 F.3d at 184–85). The court has "considerable leeway" in deciding how best to make that determination. *Kumho Tire Co., Ltd. v. Carmichael*, 526 U.S. at 152, 119 S.Ct. 1167. In determining reliability, the trial court must "focus on the principles and methodology employed by the expert, without regard to the conclusions the expert has reached or the [court's] belief as to the correctness of those conclusions." *Amorgianos v. Nat'l R.R. Passenger Corp.*, 303 F.3d 256, 267 (2d Cir. 2002). To assist courts in making this determination, the Supreme Court has identified the following factors to consider in determining the reliability of the methodology used by a proffered expert: "(1) whether the theory or technique can be tested; (2) whether the theory or technique has been subjected to peer review and publication; (3) whether the technique has a known or potential rate of error; and (4) whether the theory or technique has been met with widespread acceptance." *Emig v. Electrolux Home Prods. Inc.*, 2008 WL 4200988, *6 (S.D.N.Y. 2008) (citing *Daubert*, 509 U.S. at 593–94, 113 S.Ct. 2786). The Rule 702 inquiry is "a flexible one," *Daubert*, 509 U.S. at 594, 113 S.Ct. 2786, and while "a trial court *may* consider one or more of the more specific factors that *Daubert* mentioned[,]...[the] list of specific factors neither necessarily nor exclusively applies to all experts or in every case," *Kumho Tire Co.*, 526 U.S. at 141, 119 S.Ct. 1167. "The primary objective is 'to make certain that an expert, whether basing testimony upon professional studies or personal experience, employs in the courtroom the same level of intellectual rigor that characterizes the practice of an expert in the relevant field.' " *Cerbelli v. City of New York*, 2006 WL 2792755, *2 (E.D.N.Y. 2006) (quoting *Kumho Tire Co.*, 526 U.S. at 152, 119 S.Ct. 1167). "As the courts and Advisory Committee have made clear, 'the rejection of expert testimony is the exception rather than the rule.' " *M.B. ex rel. Scott v. CSX Transp., Inc.*, 130 F.Supp.3d 654, 665 (N.D.N.Y. 2015) (quoting Fed. R. Evid. 702, Advisory Committee's Note).

### 1. Failure to Warn Opinions

#### a. Failure to Sound Bell or Horn

Timko proposes to testify that NORAC operating rules and CSX's internal regulations required that the train's bell and horn be sounded prior to train movement. In deciding defendants' motion for summary judgment, the Court expressly considered this point and determined as a matter of law that "neither the NORAC rules nor defendants' own internal rules define defendants' duty, because those rules are more restrictive than New York's common law." (Docket # 90 at 17). The Court further found that, under New York's common law, "defendants had a duty to sound a bell or horn, upon movement of a train, to warn trespassers of the imminent danger." (*Id.* at 21). The Court explained that the duty arose because, as the evidence conclusively established, defendants had constructive knowledge of routine trespassers in the Lyons yard. (*Id.*).

***5** It is the role of the Court, and not of an expert witness, to instruct the jury on the law. In this case, the Court has already determined as a matter of law that defendants had a duty to sound a bell or horn prior to train movement, and the jury will be instructed accordingly. As a result, Timko's proposed testimony on this point simply states a legal conclusion on which the jury will be instructed, and it is thus inadmissible. *See*, *e.g.*, *United States v. Feliciano*, 223 F.3d 102, 121 (2d Cir. 2000) ("[i]n evaluating the admissibility of expert testimony, this Court requires the exclusion of testimony [that] states a legal conclusion") (internal quotation omitted); *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*, 691 F.Supp.2d 448, 476 (S.D.N.Y. 2010) (expert testimony regarding parties' legal obligations "improperly usurps the role of the trial judge in instructing the jury as to the applicable law and the role of the jury in applying the law to the facts before it").

**b. Failure to Post Warning Signs**

Timko has also offered testimony regarding defendants' alleged failure to post warning signs in the Lyons yard. Specifically, Timko has opined that good and accepted standards of practice required defendants to post signs in and around the Lyons yard stating, *e.g.*, "No Trespassing," "Private Property," and "Danger," "High Speed Trains," or other signage necessary to educate the public.

Defendants argue that Timko's opinions regarding signage are not based on accepted scientific methodology. (Docket # 65–4 at 13–14). It is well-established, however, that "expert testimony does not [have to] rest on traditional scientific methods." *United States v. Litvak*, 808 F.3d 160, 180 n.25 (2d Cir. 2015) (internal quotation omitted). "Experts of all kinds tie observations to conclusions through the use of what Judge Learned Hand called 'general truths derived from...specialized experience.' " *Kumho Tire Co.*, 526 U.S. at 148–49, 119 S.Ct. 1167 (quoting Learned Hand, *Historical and Practical Considerations Regarding Expert Testimony*, 15 Harv. L. Rev. 40, 54 (1901)). The Second Circuit has cautioned that "district courts must be mindful that the *Daubert* factors do not all necessarily apply even in every instance in which reliability of scientific testimony is challenged, and in many cases, the reliability inquiry may instead focus upon personal knowledge and experience of the expert." *United States v. Litvak*, 808 F.3d at 180 n.25 (internal quotation omitted).

Here, it is undisputed that Timko has nearly 50 years' experience in the railroad industry. He testified at his deposition that, in his experience, it was standard practice in the railroad industry to post warning signs. This is a proper expert opinion. *See Corneli v. Adventure Racing Co., LLC*, 2015 WL 4716285, *8 (N.D.N.Y. 2015) (proposed expert with long career in amusement and entertainment safety industry could properly opine on "usage, placement, and verbiage of warning signs" at go-kart track). The average juror is unlikely to have any knowledge regarding standard practice in the railroad industry regarding the posting of warning signs and would be aided by Timko's testimony on this issue. *See Scott v. City of New York*, 591 F.Supp.2d 554, 563 (S.D.N.Y. 2008) (expert with lengthy career in policing could testify about police industry practices, as such testimony was likely to aid the jury).

Defendants have argued that Timko's testimony regarding the failure to post warning signs should be excluded because it is based on faulty factual assumptions—namely, that Timko does not actually know what signs were posted in the Lyons yard at the time of Moody's accident. "Arguments about the assumptions and data underlying an expert's testimony go to the weight, rather than the admissibility, of that testimony." *Arista Records LLC v. Lime Grp. LLC*, 2011 WL 1674796, at *7; *see also Amorgianos v. Nat'l R.R. Passenger Corp.*, 303 F.3d at 266 (lack of "textual support" for expert's opinion in published studies or scientific literature may affect weight and not admissibility). Defendants may cross-examine Timko on the factual assumptions underlying his opinions about their failure to post warning signs, but they have not established that the opinions should be excluded.

***6** At oral argument, defendants' counsel advanced the additional argument that, based on the Court's summary judgment decision, Timko's opinions are not relevant because they do address the issue whether warning signs would have informed Moody that trains in the Lyons yard moved at nighttime without warning. Timko's expert report identifies the following as one of his expert opinions: "CSX failed to properly post the Lyons, NY area with signs indicating potential dangers or hazards to the public prior to the June 2006 injury to Ms. Moody." (Docket # 65–2 at 10). At his deposition, Timko

stated that the warning signs in the Lyons yard could have included "any kind of signage" and that it was incumbent on CSX to educate the public about the dangers of moving trains. (Docket # 65–3 at 157–59). Timko reiterated in his affidavit that good and accepted standards of practice required defendants to post signs in the Lyons yard "to serve as a warning to pedestrians about dangers in the Yard that they may not appreciate." (Docket # 69–5 at ¶ 16). In my estimation, these opinions are relevant to the claims remaining in this case and will be helpful to the jury in ascertaining whether the presence of warning signs in the Lyons yard would have contributed to Moody's appreciation of the danger that trains move without warning at nighttime.

**2. Other Opinions**

In his expert report and/or in his deposition testimony, Timko opined that CSX failed to sponsor Operation Lifesaver events or work with local police to educate the public, failed to properly respond to reports of pedestrian traffic at the Lyons yard, failed to properly train its employees regarding the collection and preservation of evidence, failed to perform proper airbrake testing, failed to erect a fence or barricade, and failed to properly inspect the railcars (collectively, the "non-failure to warn opinions"). (Docket ## 65–2 at 10–11; 65–3 at 148–49, 180). Timko also opined at his deposition that Moody did not appreciate the dangers inherent in climbing under a railcar. (Docket # 65–3 at 138–39). At oral argument, Moody's counsel conceded that, because the only two remaining claims in this matter relate to defendants' alleged failure to sound the horn or bell prior to train movement and failure to post warning signs, Timko's opinions are relevant only as they relate to those two specific issues. Accordingly, the Court grants defendants' motion to preclude the non-failure to warn opinions. *See In re Refco Inc. Sec. Litig.*, 2012 WL 7007795, *4 (S.D.N.Y. 2012) ("[t]o the extent the experts here are opining about the merits of dismissed claims, they fail the *Daubert* 'fit' requirement for the simple reason that those merits have already been determined and are no longer relevant to the proceedings") (collecting cases), *report and recommendation adopted*, 2013 WL 452400 (S.D.N.Y. 2013).

Defendants have also met their burden of showing that Timko is unqualified to opine as to plaintiff's particular appreciation of the dangers of climbing beneath a railcar. Timko does not purport to have any training or expertise in the fields of psychology or sociology, nor does the record suggest that he is qualified to assess Moody's particular ability to appreciate danger. "[A]n expert must...stay within the reasonable confines of his subject area, and cannot render expert opinion on an entirely different field or discipline." *M.B. ex rel. Scott v. CSX Transp., Inc.*, 130 F.Supp.3d at 672 (internal quotation omitted) (finding railroad expert unqualified to opine on minimum time required for individual to clear path of train because he was not an expert in "human factors analysis").

In sum, defendants' motion to exclude is denied with respect to Timko's proposed testimony on defendants' alleged failure to post warning signs and is granted in all other respects.

**II. Moody's Motion for Sanctions**

**A. Factual Background**

The train that injured Moody was designated Q627 and operated by engineer Frederick Albrecht. (Docket # 68–6 at 44). The locomotive attached to Train Q627 was equipped with an event recorder, also known as a "black box," which records all movements from the locomotive, including acceleration, deceleration, speed, air pressure, braking, and use of the bell and/or horn. (*Id.* at 9–11). The event recorder operates continuously. (*Id.* at 12).

***7** Michael Lewandowski ("Lewandowski"), CSX's road foreman of engines, was deposed on February 28, 2011, and testified that he had received approximately two months of on-the-job training regarding retrieval of information from an event recorder. (*Id.* at 13). Lewandowski further testified that he attended "a handful" of eight-hour classes on the same subject. (*Id.* at 14–15).

In 2006, Lewandowski was responsible for downloading information from event recorders. (*Id.* at 16). He described the process as consisting of (1) entering the locomotive; (2) measuring the wheel to determine speed; (3) ringing the bell and blowing the horn and matching the time on his cell phone to the time on the locomotive; and, (4) turning on the computer and entering the data, finding "the program," plugging in cables, and "click[ing] on the program," which would then "automatically download[ ]

to the computer." (*Id.* at 17). Lewandowski testified that he would use a laptop owned and provided by CSX to download information from an event recorder and that this laptop was not available for anyone else's use. (*Id.* at 22–23). The downloaded information from a locomotive such as the one attached to Train Q627 would consist of three files, a .STA file, a .SIS file, and a .DAT file, all of which are necessary in order to read the data. (*Id.* at 50–52).

In June 2006, Lewandowski was responsible for accessing the event recorder on the train that had injured Moody. (*Id.* at 43–45). Lewandowski had no specific memory of having downloaded the information from Train Q627, but testified that it was his practice to open the data files and confirm that the necessary data was present. (*Id.* at 52). Defendants have submitted a declaration from Stephen Swanson ("Swanson"), a senior software engineer for CSX, the exhibit to which shows that Lewandowski downloaded the data from Train Q627 at 2:30 a.m. on June 16, 2006, shortly after the accident occurred. (Docket # 81–2, Ex. A).

After retrieving data from an event recorder, Lewandowski was required by CSX's procedures to transmit it to a central data vault (the "Vault") in Jacksonville, Florida, using a communications program known as ERAD. (Docket # 68–6 at 29–30). He would select the individual data files from the downloads folder on his laptop's hard drive and transmit them to the Vault via ERAD. (*Id.*).

As discussed further below, defendants have been unable to produce the .DAT file from the event recorder on Train Q627. Lewandowski testified that he did not remember if he had uploaded the .DAT file to the Vault and that it was possible he sent only two files. (*Id.* at 52–53). CSX's records show that Lewandowski uploaded three files, but that he uploaded a .HDR file instead of a .DAT file. (Docket # 81–2, Ex. A). A .HDR file is generated by event recorders on a different kind of locomotive than the one involved in the instant matter. (*Id.* at ¶ 11). Defendants surmise that Lewandowski inadvertently selected the .HDR file rather than the correct .DAT file as the third file in his upload. (Docket # 81 at 5).

At some point between Moody's accident in June 2006 and 2010, the laptop Lewandowski used to download the files from Train Q627's event recorder crashed. (Docket # 68–6 at 54). Lewandowski estimated that the crash occurred "within a year or two" of Moody's accident. (*Id.* at 54–55). Lewandowski sent the crashed laptop to Jacksonville. (*Id.* at 57–58). Defendants are unable to provide information regarding what efforts, if any, were made to recover data from the crashed laptop, nor have they been able to produce the laptop. (*See* Docket # 81 at 5).

***8** Moody served discovery demands on June 23, 2009, in which she requested, among other items, the "[c]omplete event recorder printout(s) for [Train Q627]." (*See* Docket ## 22 at 1; 68–3 at 15). In their response dated April 9, 2010, defendants stated that they had "identified a download for the subject locomotive" but "[t]he data...is not in readable format" and that they were "seeking outside expert assistance in attempting to retrieve the data from the download." (Docket # 68–3 at 15). On April 14, 2010, Moody served a supplemental notice to produce "specifically requesting the 'download' and information/software necessary to interpret the data." (*See* Docket # 22 at 1). On June 22, 2010, defendants responded to Moody's supplemental notice by enclosing a copy of the 'download' and reiterating that they had been unable to "discern the format or obtain any readable information." (Docket # 68–4 at 1–2). Defendants' counsel also sent a letter dated June 22, 2010, in which he stated that Lewandowski had downloaded the data from the event recorder and:

> It appears Mr. Lewandowski downloaded two of three files necessary to read the information, apparently failing to upload a "dat" file. Upon discovery of the missing "dat" file, inquiry was made of Mr. Lewandowski to kindly check his laptops to determine if the missing file was available. Unfortunately, by the time this request was made, Mr. Lewandowski's laptop had crashed and [been] turned into CSX Communications for recycling and/or destruction.

(Docket # 68–5 at 1).

**B. The Parties' Positions**

Moody seeks sanctions on the grounds that defendants have spoliated evidence. (Docket # 68–1 at 11).

Specifically, Moody maintains that defendants spoliated the data from the event recorder and requests that the Court strike defendants' answer or, in the alternative, provide an adverse inference instruction. (*Id.*).

According to Moody, defendants had a duty to preserve the event recorder data saved on Lewandowski's laptop and in the Vault. (Docket # 68–1 at 14). Moody argues that defendants were aware that the event recorder data was "central" to the parties' dispute and that the laptop at issue was "the only tangible piece of evidence that held this critical data," and thus they had a duty to preserve the evidence. (*Id.* at 15). Moody further contends that defendants failed to take reasonable steps to preserve the data on the laptop and/or in the Vault and their actions were willful or grossly negligent. (*Id.* at 16–17). Finally, Moody argues that she has been prejudiced by the destruction of the data because it would have conclusively resolved the central issue of whether the locomotive's horn or bell sounded prior to train movement. (*Id.* at 19–20). Accordingly, she maintains that severe sanctions are warranted. (*Id.* at 20).

Defendants dispute that sanctions are warranted, maintaining that they took reasonable steps to preserve the event recorder data, Moody was not prejudiced by the loss of the data, and defendants did not act culpably. (*See* Docket # 81 at 9). Defendants characterize their actions (sending Lewandowski to retrieve the event recorder data within hours of the accident and promptly sending it to a central system) as objectively reasonable and urge the Court to find that only "inadvertent human error" caused the loss of the data. (*Id.* at 10). Defendants further contest that they had any obligation to preserve Lewandowski's laptop, emphasizing that the law does not require parties to maintain multiple copies of relevant evidence. (*Id.* at 11).

Defendants argue that Moody has not been prejudiced by the loss of the event recorder data because (1) failure to sound the bell or horn would not amount to negligence (*id.* at 13), and (2) Moody may still present her claim to the jury without the event recorder data, and the jury will be "perfectly capable of determining who is telling the truth" about whether or not the horn or bell was sounded (*id.* at 14–15). Defendants contend that there is no way of knowing whether the event recorder data would have supported Moody's version of events, and "[i]t is at least as likely that the event recorder data would have corroborated the engineer's (Mr. Albrecht's) testimony that he *did* sound the horn." (*Id.* at 15) (emphasis in original).

***9** Finally, defendants maintain that, even if the Court were to determine that some sanction is appropriate, severe sanctions are precluded because they did not intentionally deprive Moody of the event recorder data. (*Id.* at 16). Defendants contend that simple human error amounts "at most to simple negligence" and does not constitute bad faith or intentional destruction of evidence. (*Id.* at 17).

In reply, Moody argues that the data at issue was lost not because of isolated human error, but due to multiple and "monumental" failures on the part of defendants to ensure that the data remained accessible, from which the Court may infer that defendants intentionally deprived her of the event recorder data. (Docket # 83 at 5–6, 10–11). Moody further maintains that she was indeed prejudiced by the loss because the data would have conclusively determined whether the horn was sounded. (*Id.* at 6–7). In the alternative, Moody asks the Court to impose "other curative sanctions." (*Id.* at 11–12). [3]

**C. Analysis**

"Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999). "The right to impose sanctions for spoliation arises from a court's inherent power to control the judicial process and litigation, but the power is limited to that necessary to redress conduct 'which abuses the judicial process.' " *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec.*, 685 F.Supp.2d 456, 465 (S.D.N.Y. 2010) (internal quotation omitted), *abrogated on other grounds by Chin v. Port Auth. of New York & New Jersey*, 685 F.3d 135 (2d Cir. 2012), *cert. denied*, 569 U.S. 904, 133 S.Ct. 1724, 185 L.Ed.2d 785 (2013).

Generally, a party bringing a spoliation motion must demonstrate that: (1) the party charged with destroying the evidence had an obligation to preserve it; (2) the records were destroyed with a "culpable state of mind"; and, (3) the destroyed evidence was relevant to the party's claim or defense. *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 107 (2d Cir. 2002)

(citing *Byrnie v. Town of Cromwell, Bd. of Educ.*, 243 F.3d 93, 107–08 (2d Cir. 2001)); *see also Arista Records LLC v. Usenet.com, Inc.*, 608 F.Supp.2d 409, 430 (S.D.N.Y. 2009); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 220 (S.D.N.Y. 2003). This general rule applied to the destruction of both tangible and electronic evidence until December 1, 2015, at which time Rule 37 of the Federal Rules of Civil Procedure was amended to provide a different standard for destruction of electronically stored information. Specifically, Rule 37(e) now provides:

> If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:
>
> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> ***10** (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> (A) presume that the lost information was unfavorable to the party;
>
> (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
>
> (C) dismiss the action or enter a default judgment.

Fed. R. Civ. P. 37(e). This new rule "rejects cases such as *Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99 (2d Cir. 2002), that authorize the giving of adverse-inference instructions on a finding of negligence or gross negligence." *McIntosh v. United States*, 2016 WL 1274585, *31 (S.D.N.Y. 2016) (internal quotation omitted).

Rule 37(e) was amended as part of the 2015 amendments to the Federal Rules of Civil Procedure, and the new version "govern[s] in all proceedings in civil cases commenced after December 1, 2015, and, insofar as just and practicable, all proceedings pending on that date." *Id.* (internal quotations omitted). "Courts within this Circuit have applied the amended version of Rule 37(e) on a case-by-case basis." *Distefano v. Law Offices of Barbara H. Katsos, PC*, 2017 WL 1968278, *4 (E.D.N.Y. 2017). With some exceptions, motions that were filed and briefed prior to December 1, 2015, have been decided under the prior standard, and those briefed thereafter have been decided under the amended version. *See id.*(collecting cases).

Here, the Court finds that it is both just and practicable to apply the current version of Rule 37(e) to Moody's motion. The motion was filed on April 1, 2016, four months after the 2015 amendments took effect. Moreover, both parties' briefs acknowledge and argue the current version of Rule 37(e). Additionally, "[t]he new rule places no greater substantive obligation on the party preserving ESI" and "is in some respects more lenient as to the sanctions that can be imposed for violation of the preservation obligation," and therefore "there is no inequity in applying it." *CAT3, LLC v. Black Lineage, Inc.*, 164 F.Supp.3d 488, 496 (S.D.N.Y. 2016).

Moody argues that the current version of Rule 37(e), which deals only with the loss of electronically stored information, does not apply to defendants' destruction of Lewandowski's "crashed" laptop because it is tangible evidence. (*See* Docket # 83 at 3–6). I disagree. Although the laptop itself is tangible evidence, the electronic information stored within the laptop is the relevant evidence. Had defendants lost or destroyed the contents of the laptop but preserved the physical hardware, Moody would be in precisely the same position as she is now. It is the loss of the electronic evidence stored on the laptop that gives rise to this dispute—one that falls squarely within the scope of Rule 37(e), the terms of which apply whenever "electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it." Fed. R. Civ. P. 37(e).

Accordingly, this Court will apply the current version of Rule 37(e). Under that rule, the Court must consider (1) whether electronic information that should have been preserved has been lost; (2) whether defendants took "reasonable steps" to preserve that information; (3) whether the information can be restored or replaced through additional discovery;

***11** (4) whether Moody has been prejudiced by the loss of the information; and, (5) whether defendants acted with the intent to deprive Moody of the information's use. *See generally CAT3, LLC v. Black Lineage, Inc.*, 164 F.Supp.3d at 495–502.

**1. Duty to Preserve**

"Identifying the boundaries of the duty to preserve involves two related inquiries:
*when* does the duty to preserve attach, and *what* evidence must be preserved?" *Zubulake v. UBS Warburg LLC*, 220 F.R.D. at 216 (emphasis in original). A party is obligated to preserve evidence when it has "notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." *Fujitsu Ltd. v. Fed. Express Corp.*, 247 F.3d 423, 436 (2d Cir.), *cert. denied*, 534 U.S. 891, 122 S.Ct. 206, 151 L.Ed.2d 146 (2001); *Creative Res. Grp. of New Jersey, Inc. v. Creative Res. Grp., Inc.*, 212 F.R.D. 94, 105 (E.D.N.Y. 2002). Here, defendants do not contest that they had an obligation to preserve the event recorder data, nor could they plausibly do so. No genuine question exists that the event recorder data from the locomotive involved in the accident that injured the plaintiff likely contains relevant information. Nor is there any dispute that the data has been lost. Accordingly, the Court finds that the first element of Rule 37(e) has been met.

**2. Reasonable Steps to Preserve**

Moody, as the party seeking sanctions, must show that defendants failed to take reasonable steps to preserve the event recorder data. Moody maintains that defendants' failure at any time between 2006 and 2010 to confirm that the files uploaded to the Vault by Lewandowski were complete and accessible was unreasonable. Moody further contends that destruction of the crashed laptop was unreasonable.

As a threshold matter, I find that defendants' explanation for the loss of the data strains credulity. According to defendants, although Lewandowski uploaded certain event recorder data to the Vault within hours of Moody's accident, no one attempted to access or review the data at any time during the next four years, despite the fact that defendants had been sued by the injured party and the data—had it been uploaded correctly—would have established relevant and material facts, such as: (1) whether the bell and/or horn were sounded prior to train movement; (2) how fast the train was moving when Moody was struck; and, (3) whether the brakes had been applied. The proposition that a sophisticated railroad transportation corporation such as CSX could be involved in a serious accident in which an individual lost a limb and thereafter fail for four years to review critical data relating to how that accident occurred is unfathomable. The implausible nature of defendants' narrative is heightened by their complete inability to explain what happened to Lewandowski's laptop after he returned it to Jacksonville. Of course, a court is not required to credit explanations for the loss of the relevant evidence that it finds incredible. *See*, *e.g.*, *Babaev v. Grossman*, 2008 WL 4185703, *3 (E.D.N.Y. 2008) (imposing sanctions for spoliation where "the court d[id] not find the defendants' arguments credible, nor their evidence persuasive, on the fundamental issue of whether they engaged in spoliation of the evidence on the...computer").

***12** Even if defendants' explanation for the loss of the data were credited, their failure to access the files uploaded to the Vault for the four-year period before 2010 conflicted with their duties under the Federal Rules of Civil Procedure. The instant lawsuit was commenced in July 2007 and removed to federal court in August of that year. (*See* Docket # 1). Moody's complaint expressly asserts that the train that injured her "began moving without issuing a siren, signal or any warning whatsoever." (Docket # 1–3 at ¶ 17). In their answer, filed on August 22, 2007, defendants denied that allegation "for lack of knowledge or information sufficient to form a belief as to [its] truth." (Docket # 2 at ¶ 17). Pursuant to Rule 11 of the Federal Rules of Civil Procedure, a party or attorney who signs a pleading "certifies that to the best of the person's knowledge, information, and belief, *formed after an inquiry reasonable under the circumstances*[,]...the denials of factual contentions are warranted on the evidence or, if specifically so identified, are reasonably based on belief or lack of information." Fed. R. Civ. P. 11(b)(4) (emphasis added). Accepting defendants' recitation of events, they submitted an answer —which they allowed to stand without supplementation —denying for lack of knowledge that the involved train moved without sounding the bell and/or horn without checking data, in their sole control and possession, that they knew would have conclusively shown whether that was accurate. Although Moody has not sought Rule 11 sanctions and this Court is not determining that issue, defendants' apparent failure to conduct the inquiry required by Rule 11 is relevant to this Court's assessment of defendants' conduct.[4] Significantly, had defendants

reviewed the event recorder data prior to submission of their answer (or promptly thereafter in order to supplement it), they would have discovered that the .DAT file was missing no later than August 2007. According to Lewandowski's testimony, the file likely still existed on his laptop at that time and could have been recovered. (Docket # 68–6 at 54–55).

Defendants also failed to comply with their obligation under Rule 26 to provide "without awaiting a discovery request...a copy—or a description by category and location—of all documents, *electronically stored information*, and tangible things that [they had] in [their] possession, custody, or control and may use to support [their] claims or defenses." Fed. R. Civ. P. 26(a)(1)(A)(ii) (emphasis added). Initial disclosures must be "based on the information then reasonably available to [the party]." Fed. R. Civ. P. 26(a)(1)(E). Moreover, discovery responses must be based on a "reasonable inquiry." *Markey v. Lapolla Indus., Inc.*, 2015 WL 5027522, *15, 19 (E.D.N.Y. 2015) (sanctioning law firm for failing "to conduct a more thorough investigation of the discovery in [p]laintiffs' possession prior to serving the [i]nitial [d]isclosures"), *report and recommendation adopted*, 2016 WL 324968 (E.D.N.Y. 2016). Pursuant to this Court's scheduling order, the Rule 26 mandatory disclosures were required to be made by no later than July 15, 2008. (Docket # 6). Again, even accepting defendants' representations about what they did and what they knew about the data, they nonetheless submitted their initial disclosures without apparently reviewing the event recorder data, despite the fact that Moody's complaint undeniably put them on notice that whether or not the bell and/or horn were sounded prior to the train's movement was a key factual dispute. Considering all the circumstances, this Court finds that defendants' failure to perform this straightforward and required inquiry was unreasonable, at best. *Cf. Tippett v. Burlington N. Santa Fe Corp.*, 2009 WL 10665811, *2 (D.N.M. 2009) (noting train event recorder was provided with initial disclosures), *aff'd in part, vacated in part sub nom. Henderson v. Nat'l R.R. Passenger Corp.*, 412 Fed.Appx. 74 (10th Cir. 2011); *BNSF Ry. Co. v. LaFarge Sw., Inc.*, 2008 WL 9471222, *1 (D.N.M. 2008) (same).

Moreover, [a] party's failure to maintain electronic data in an accessible format may constitute sanctionable conduct. *See*, *e.g.*, *Mazzei v. Money Store*, 308 F.R.D. 92, 101 (S.D.N.Y. 2015) (failure to maintain invoice system in accessible format warranted sanctions), *aff'd*, 829 F.3d 260 (2d Cir. 2016), *cert. denied*, —— U.S. ——, 137 S.Ct. 1332, 197 L.Ed.2d 518 (2017); *Arrowhead Capital Fin., Ltd. v. Seven Arts Entm't, Inc.*, 2016 WL 4991623, *20 (S.D.N.Y. 2016) (delay in downloading discoverable information from server or moving it from server to new cloud-based system was reckless and unreasonable when party knew it might lose access to server), *reconsideration granted in part on unrelated grounds*, 2017 WL 1653568 (S.D.N.Y. 2017). Courts routinely hold that a party's discovery obligations include taking "affirmative steps" to "ensure that all potentially relevant evidence is retained." *Richard Green (Fine Paintings) v. McClendon*, 262 F.R.D. 284, 289 (S.D.N.Y. 2009) (internal quotation omitted) (finding spoliation where party failed to maintain original version of electronic spreadsheet, but instead transferred files from hard drive to compact discs). Here, defendants themselves admit that they took no steps to confirm that the event recorder data had been properly uploaded by Lewandowski. Indeed, according to Swanson's declaration, any attempt to access the information in the Vault would have revealed the uploading error. (*See* Docket # 81–1 at ¶ 12). In other words, defendants allowed the original data on the event recorder to be overwritten and destroyed without ensuring that it had been appropriately preserved. Just as it would be unreasonable for a party preserving a paper file to copy it blindly, put it in a drawer without ever looking at it, and then destroy the original, so too was it unreasonable for defendants to upload the event recorder data to the Vault and not even look at the files to confirm that the appropriate data had been uploaded and was accessible. This failure is especially remarkable in view of the important and irreplaceable nature of the data at issue.

***13** Referring to the copy of the event recorder data stored in the Vault as a "backup," defendants assert they had no obligation to "double-check" a backup. (*See*, *e.g.*, Docket # 85–1 at 3). To the contrary, Lewandowski's testimony makes clear that the copy in the Vault was the primary copy. (*See* Docket # 68–6 at 48–49). Specifically, he testified that any request for event recorder data would "go through Jacksonville" and he played no role in the process of disseminating event recorder data. (*Id.*). Indeed, elsewhere in their papers defendants state that they "reasonably believed that [the] primary copy of the data had been properly stored in the Jacksonville data vault." (Docket # 81 at 11). Defendants' argument that the Vault constituted a "data backup system" and that they

had no obligation to "double-check [the] backup" (*see* Docket # 85–1 at 3) is specious and does not change the Court's conclusion that it was unreasonable for defendants to fail to confirm that the uploading procedure had been properly completed.

The Court further finds that defendants acted unreasonably in destroying or recycling Lewandowski's crashed laptop. Lewandowski testified that it had crashed within a year or two after the accident and that he sent it to Jacksonville. (Docket # 68–6 at 54–55, 57–58). Defendants have been unable to locate any data that was retrieved from the crashed laptop or to provide any information regarding whether and, if so, what efforts were undertaken to retrieve such data.

Although it was decided under the prior version of Rule 37(e), the court's decision in *Learning Care Grp., Inc. v. Armetta*, 315 F.R.D. 433, 437 (D. Conn. 2016), is instructive. There, the plaintiff had a policy of backing up employee emails to a server, rather than saving them locally on a specific computer. *Id.* at 436. After litigation had been commenced, the plaintiff destroyed, in the normal course of business and consistent with its normal practices, a laptop computer used by its former chief marketing officer ("CMO"), who was a key player in the activity underlying the lawsuit. *Id.* Numerous emails sent by the former CMO were later discovered to have been deleted from the server. *Id.* The defendants moved for sanctions on the grounds that the plaintiff had spoliated evidence by destroying the laptop from which "they would likely have been able to recover many of the deleted e-mails." *Id.* at 436–37. The court agreed that the plaintiff had an obligation to preserve the laptop and that its conduct in destroying it was negligent. *Id.* at 437–40.

As in *Learning Care*, defendants destroyed or recycled Lewandowski's laptop despite knowing that it likely contained relevant evidence that they never confirmed had been properly uploaded to another repository (the Vault). For all the reasons discussed herein, I find that defendants did not take reasonable steps to preserve the event recorder data.

### 3. Reproducibility of Lost Information

The third element the Court must consider is whether the lost information can be restored or replaced by other means. Nothing in the record before the Court suggests that the event recorder data may be restored or replaced, and defendants have not argued otherwise. Accordingly, the Court concludes that this element of Rule 37(e) has been met.

### 4. Prejudice to Moody

Under Rule 37(e)(1), sanctions may be imposed where the loss of electronic information has prejudiced the moving party. Here, defendants dispute that Moody has been prejudiced, arguing that Moody has other evidence available to her regarding whether the bell and/or horn were sounded and that the event recorder data might not have supported Moody's claims.

"In order to impose a sanction under Rule 37(e)(1), the court must have some evidence regarding the particular nature of the missing ESI in order to evaluate the prejudice it is being requested to mitigate." *Eshelman v. Puma Biotechnology, Inc.*, 2017 WL 2483800, *5 (E.D.N.C. 2017). The Advisory Committee notes explain:

> The rule does not place a burden of proving or disproving prejudice on one party or the other. Determining the content of lost information may be a difficult task in some cases, and placing the burden of proving prejudice on the party that did not lose the information may be unfair. In other situations, however, the content of the lost information may be fairly evident, the information may appear to be unimportant, or the abundance of preserved information may appear sufficient to meet the needs of all parties. Requiring the party seeking curative measures to prove prejudice may be reasonable in such situations. The rule leaves judges with discretion to determine how best to assess prejudice in particular cases.

***14** Fed. R. Civ. P. 37(e) advisory committee's note to 2015 amendment. Prejudice under Rule 37(e) may be found where a party has been required to "piece together information from other sources to try to recover relevant

documents." *In re: Ethicon, Inc.*, 2016 WL 5869448, *4 (S.D. W. Va. 2016).

Under the circumstances of this case, the Court finds that it would be unreasonable and unfair to require Moody to demonstrate that the event recorder data would have been favorable to her. Indeed, the Second Circuit has cautioned district courts against "holding the prejudiced party to too strict a standard of proof regarding the likely contents of...destroyed evidence." *Kronisch v. United States*, 150 F.3d 112, 128 (2d Cir. 1998). At least one court has held that "[t]o show prejudice resulting from the spoliation [under the current version of Rule 37(e)], a party must only come forward with plausible, concrete suggestions as to what [the destroyed] evidence might have been." *TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez–Toledo*, 2017 WL 1155743, *1 (D.P.R. 2017) (internal quotations omitted) (finding prejudice where party "plausibly suggest[ed]" that a discarded laptop "might have" contained documents or information relevant to the action).

Here, as defendants' counsel acknowledged at oral argument, the event recorder data would have conclusively determined whether the horn or bell on Train Q627 were sounded prior to movement. That critical and irreplaceable data was within defendants' complete control to review and produce, but they failed to take simple, reasonable steps to preserve it. Moody has identified testimonial evidence (her own and that of her friend Tiffany Johnson) that the bell and/or horn were not sounded prior to train movement. Under these circumstances, it is plausible that the data from the event recorder would have supported Moody's case. Accordingly, prejudice has been established.

In addition, the loss of the data has required Moody to spend additional resources to attempt to resolve this critical factual dispute. Moody likely would not have deposed Lewandowski had the event recorder data been available, and the Court could have determined as a matter of law whether or not defendants had complied with their duty to sound the bell and/or horn prior to train movement. The Court therefore concludes that defendants' loss of this information has prejudiced Moody. *See*, *e.g*, *Aktas v. JMC Dev. Co.*, 877 F.Supp.2d 1, 18 (N.D.N.Y. 2012) (party's inability to inspect original evidence resulted in "significant prejudice"), *aff'd*, 563 Fed.Appx. 79 (2d Cir. 2014); *Henkel Corp. v. Polyglass USA, Inc.*, 194 F.R.D. 454, 457 (E.D.N.Y. 2000) (defendant's inability to inspect original evidence that plaintiff inspected resulted in uneven "evidentiary playing field"; "[b]ecause plaintiff is responsible for this evidentiary disparity, some form of sanction is appropriate").

**5. Intentional Deprivation**

Having determined that some sanction is appropriate in this case, the Court must decide whether the specific sanctions sought by Moody—striking defendants' answers and/or issuing an adverse inference instruction—are warranted. "Rule 37(e)[ (2) ][5] now reserves the harshest discovery sanctions, such as adverse inference instructions, dismissals, or default judgments, only for cases in which the court can 'fin[d] that the [spoliating] party acted with the intent to deprive another party of the information's use in the litigation.' " *Jenkins v. Woody*, 2017 WL 362475, *17 (E.D. Va. 2017) (quoting Fed. R. Civ. P. 37(e)(2)). This intent standard is "stringent" and "does not parallel other discovery standards." *Id.*

***15** Moody argues that the Court may infer an intent to deprive from defendants' actions in this matter. (*See* Docket # 68–1 at 22). The Court agrees. In *Ala. Aircraft Indus., Inc. v. Boeing Co.*, 319 F.R.D. 730 (N.D. Ala. 2017), the court held that a party may be found to have acted with an intent to deprive within the meaning of Rule 37(e)(2) where "(1) evidence once existed that could fairly be supposed to have been material to the proof or defense of a claim at issue in the case; (2) the spoliating party engaged in an affirmative act causing the evidence to be lost; (3) the spoliating party did so while it knew or should have known of its duty to preserve the evidence; and (4) the affirmative act causing the loss cannot be credibly explained as not involving bad faith by the reason proffered by the spoliator." *Id.* at 746 (quoting *Managed Care Solutions, Inc. v. Essent Healthcare, Inc.*, 736 F.Supp.2d 1317, 1323 (S.D. Fla. 2010)). Defendants' conduct in this case supports such an inference. As explained more fully *supra*, no question exists that the lost evidence was highly relevant—if not the most important objective evidence—to the determination of liability. While knowing they had a duty to preserve the event recorder data, defendants allowed the original data on the event recorder to be overwritten, and destroyed or recycled Lewandowski's laptop without ever confirming

that the data had been preserved in another repository. Finally, their failure to make any effort over the course of four years to confirm that the data was properly preserved in the Vault undercuts the reasonableness and credibility of their asserted belief that the material was still accessible. On this record, the Court finds that defendants acted with the intent to deprive Moody of the use of the event recorder data. *See id.* at 746 ("this...unexplained, blatantly irresponsible behavior leads the court to conclude that [defendant] acted with the intent to deprive [plaintiff] of the use of this information"). *See also Brown Jordan Int'l, Inc. v. Carmicle*, 2016 WL 815827, *1, 33–37 (S.D. Fla. 2016) (finding intent to deprive where spoliating party did not credibly explain failure to preserve), *aff'd*, 846 F.3d 1167 (11th Cir. 2017); *Internmatch, Inc. v. Nxtbigthing, LLC*, 2016 WL 491483, *1, 4 n.6, 11 (N.D. Cal. 2016) (finding defendants had acted with intent to deprive where "the alleged chronology of events [was] highly improbable, [and] [d]efendants' story [was] filled with inconsistencies."

Moreover, even accepting as credible defendants' explanation for the loss of the event recorder data, this Court still concludes that defendants' actions presented sufficient circumstantial evidence from which to infer that they intended to deprive Moody of the relevant data. *See Ottoson v. SMBC Leasing & Fin., Inc.*, 2017 WL 2992726, *9 (S.D.N.Y. 2017) (intentional failure to take steps necessary to preserve relevant evidence "satisfies the requisite level of intent required by Federal Rule of Civil Procedure 37(e)"). Here, even if Lewandowski's initial error in uploading the event recorder data to the Vault is excused, defendants' repeated failure over a period of years to confirm that the data had been properly preserved despite its ongoing and affirmative Rule 11 and Rule 26 obligations, particularly before discarding Lewandowski's laptop, is so stunningly derelict as to evince intentionality. *See*, *e.g.*, *Henkel Corp. v. Polyglass USA, Inc.*, 194 F.R.D. at 457 (plaintiff's conduct in disregard of its discovery obligations, while suggesting but not conclusively establishing bad faith, demonstrated that it was "highly culpable for the destruction of the relevant evidence") (citing *Shaffer v. RWP Grp., Inc.*, 169 F.R.D. 19, 26 (E.D.N.Y. 1996) (finding party "highly culpable" for its "conscious and reckless disregard" of discovery obligations)). Thus, because I find that defendants' acted with intent to deprive, Rule 37(e)(2) permits the imposition of severe sanctions.

Contrary to Moody's position, this Court does not find that an order striking defendants' answer is justified. "[C]ourts must be wary of issuing case-dispositive sanctions; such sanctions should be imposed only in extreme circumstances, usually after consideration of alternative, less drastic sanctions." *Arista Records LLC v. Usenet.com, Inc.*, 633 F.Supp.2d 124, 141 (S.D.N.Y. 2009) (internal quotation omitted). Here, although defendants' actions were sufficiently egregious to support a finding of intent, they were not so outrageous as to warrant outright disposition of the case. Rather, in my estimation, an adverse inference instruction is justified. "The prophylactic and punitive rationales [for an adverse inference instruction] are based on the...commonsensical proposition that the drawing of an adverse inference against parties who destroy evidence will deter such destruction, and will properly place the risk of an erroneous judgment on the party that wrongfully created the risk." *Kronisch v. United States*, 150 F.3d at 126 (internal quotation omitted). Here, an adverse instruction appropriately addresses the evidentiary gap caused by defendants' loss of such material evidence. The precise form of the instruction will be decided by the Court at the time of trial.

## III. Defendants' Motion to Bifurcate the Trial

### A. Factual Background

***16** As a result of the accident, Moody suffered extensive injuries, including the "traumatic amputation of her left leg, as well as severe and extensive damage to and disfigurement of her right leg, including the loss of the great toe on her right foot." (Docket # 98–2 at 3). According to defendants, Moody intends to call at least three damages experts at trial, in addition to the physicians who treated her injuries. (Docket # 98–1 at ¶¶ 11–13). Defendants state that they will likely introduce testimony of other medical and economics experts in order to defend against Moody's claimed damages and, other than testimony from Moody herself, there is unlikely to be an overlap between liability witnesses and damages witnesses. (*Id.* at ¶¶ 14–15).

### B. The Parties' Positions

Defendants request that the Court bifurcate the trial into a liability phase and a damages phase. (Docket # 98–3 at 1). Defendants contend that bifurcation will simplify the issues and likely expedite the proceedings because the jury

is likely to find in their favor on the issue of liability. (*Id.* at 2–4). Defendants further argue that there is a risk of juror confusion absent bifurcation. (*Id.* at 4–6). Finally, defendants advance the novel argument that bifurcation is mandated by the Due Process Clause. (*Id.* at 6–8).

Moody contends that the risk of undue prejudice is low and speculation about juror sympathy is insufficient to warrant bifurcation. (Docket # 103–1 at 5–6). Moody further contends that "any potential for prejudice may be avoided through appropriate jury instructions." (*Id.* at 8). She points out that her physical injuries are obvious, and bifurcation will not prevent the jury from feeling sympathy for her. (*Id.*). If anything, bifurcation could prejudice her because the jury may reasonably infer, and be influenced by the assumption, that their term of jury service will be shortened by a liability verdict in favor of defendants. (*Id.* at 11).

Moody further opposes defendants' motion on the basis that the issues of liability and damages are intertwined. (*Id.* at 12–13). According to Moody, because her theory of the case presupposes that she would have had time to escape from beneath the train had defendants sounded the horn or bell prior to movement, "the biomechanics of her injuries, and the nature in which they were sustained, are critical to liability." (*Id.* at 13).

### C. Analysis

"Decisions to bifurcate trials...are authorized by Federal Rule of Civil Procedure 42(b) and are typically well within the discretion of district courts." *In re Sept. 11 Litig.*, 802 F.3d 314, 339 (2d Cir. 2015). Under Rule 42(b), bifurcation may be ordered "[f]or convenience, to avoid prejudice, or to expedite and economize." Fed. R. Civ. P. 42(b); *see also Vichare v. AMBAC Inc.*, 106 F.3d 457, 466 (2d Cir. 1996) ("[t]he interests served by bifurcated trials are convenience, negation of prejudice, and judicial efficiency"). Bifurcation is "the exception, not the rule, and the movant must justify bifurcation on the basis of the substantial benefits that it can be expected to produce." *Svege v. Mercedes–Benz Credit Corp.*, 329 F.Supp.2d 283, 284 (D. Conn. 2004); *see also Kos Pharm., Inc. v. Barr Labs., Inc.*, 218 F.R.D. 387, 391 (S.D.N.Y. 2003) ("[t]he inconveniences, inefficiencies and harms inherent in these probable consequences [of bifurcation]—to the parties and third parties, to the courts, and to the prompt administration of justice—weigh against separation of trials and suggest that, for those probable adverse effects to be overcome, the circumstances justifying bifurcation should be particularly compelling and prevail only in exceptional cases"). In considering whether to bifurcate, "the [c]ourt should examine, among other factors, whether bifurcation is needed to avoid or minimize prejudice, whether it will produce economies in the trial of the matter, and whether bifurcation will lessen or eliminate the likelihood of juror confusion." *Svege v. Mercedes–Benz Credit Corp.*, 329 F.Supp.2d at 284. For the reasons set forth below, the Court finds that bifurcation is not appropriate.

#### 1. Minimization of Prejudice

***17** Defendants argue that they will be prejudiced if the trial is not bifurcated because evidence of Moody's damages will "dilute[ ] the proof on liability" and will also "create[ ] the risk that a jury will return a liability verdict that is tainted by the damages evidence and the sympathy Ms. Moody's injuries are likely to invoke." (Docket # 98–3 at 5–6). These concerns do not warrant bifurcation. While Moody's injuries may evoke some sympathy in the jurors, "the same observation could be made in any case involving traumatic injuries or death. Yet, the issues of liability and damages are routinely tried [together], even in cases of death or severe injury." *Svege*, 329 F.Supp.2d at 284; *see also Chase v. Near*, 2007 WL 2903823, *2 (W.D.N.Y. 2007) (denying bifurcation motion where "there are no particular factors specific to this case that distinguish the potential for prejudice here from the potential prejudice which is normally and customarily dealt with through an appropriate charge and curative instructions where necessary") (internal quotation omitted). Moody's injuries, while serious, do not raise an unusual risk of juror sympathy. In any event, regardless of whether the Court bifurcates the issues of liability and damages, the jurors will inevitably learn in the liability phase that Moody was seriously injured. "Therefore, it is not clear to this [c]ourt that bifurcation will eliminate or even substantially reduce the potential prejudice that [d]efendants fear." *Svege*, 329 F.Supp.2d at 285 (finding bifurcation inappropriate where jurors would inevitably learn during liability phase that father had died and two children had been injured in accident). Moreover, "[a]ny danger of prejudice c[an] be minimized through appropriate jury instructions." *Ake v. Gen. Motors Corp.*, 942 F.Supp. 869, 877 (W.D.N.Y. 1996) (collecting cases); *see also Coyle v. Crown Enters., Inc.*, 2009 WL 2399904,

*1 (W.D.N.Y. 2009) ("concern that the presentation of substantial evidence regarding [p]laintiffs' injuries could somehow prejudice and confuse the jury can be obviated through a curative jury instruction").

### 2. Promotion of Judicial Economy

Defendants also argue that "there is a substantial likelihood that bifurcation here will avoid the need for damages testimony altogether" and that "[t]he probability of a defense verdict on liability is especially high in this case." (Docket # 98–3 at 3). "Defendants' argument that they are likely to succeed at the liability stage, thereby eliminating the need for a second trial, is not persuasive. This argument could be made in every case." *Mensler v. Wal–Mart Transp., LLC*, 2015 WL 7573236, *4 (S.D.N.Y. 2015); *see also Svege*, 329 F.Supp.2d at 285 ("[t]he [c]ourt certainly appreciates [d]efendants' confidence on the eve of trial[;] [h]owever, without expressing any view on the ultimate outcome of this trial, it suffices to say that [d]efendants' projected savings are by no means guaranteed") (internal quotation omitted). Although the Court noted that the summary judgment determination in this case was close, "[t]he [c]ourt cannot predict who will be successful at the liability stage, and therefore this argument does not justify bifurcation." *Mensler v. Wal–Mart Transp., LLC*, 2015 WL 7573236, at *4. Considering that this case has been pending for nearly a decade, the potential, but far-from-certain, benefit to judicial economy created by a bifurcated trial does not justify the delay, however modest it may be, in a final resolution of the case. In addition, a decision to bifurcate may create unnecessary disputes about the admissibility of particular evidence during the liability phase—the argument and resolution of which may prolong the jury's ultimate determination.

### 3. Prevention of Juror Confusion

Defendants contend that there is no genuine risk of evidentiary overlap between the issues of liability and damages. I disagree. As Moody correctly points out, one of the key disputes as to liability is whether defendants' alleged failure to sound the locomotive's bell and/or horn proximately caused Moody's injuries. Moody therefore intends to offer evidence that she would have been able to escape from underneath the train without injury if the bell and/or horn had sounded. This proof will likely encompass evidence concerning how Moody's injuries occurred, including which parts of the train impacted which parts of her body. In addition, Moody and Tiffany Johnson will both testify on the issues of liability and damages. Under these circumstances, bifurcation is not warranted. *See*, *e.g.*, *Ake v. Gen. Motors Corp.*, 942 F.Supp. at 877 (bifurcation not warranted where "[s]ome evidence, such as that relating to the fire, would be relevant to both liability (to show the cause of death) and damages for conscious pain and suffering"); *Mensler*, 2015 WL 7573236, at *4 ("[t]he evidence in this matter regarding liability and damages, while separate and potentially severable, overlaps[;] [f]or example, [two witnesses] will testify to both liability and damages"); *Chase v. Near*, 2007 WL 2903823, at *2 (bifurcation is inappropriate where "there will necessarily be some overlap of witnesses and their testimony").

***18** Moreover, "this case does not present complex legal or factual questions" (*Mensler*, 2015 WL 7573236, at *4), and no reason exists to doubt a jury's inability to separate the issues of liability and damages. *See also Svege*, 329 F.Supp.2d at 283 ("this case is not so complicated and the liability issues are not so numerous or complex that the jury is likely to be distracted from their task on liability by the presence of testimony and exhibits relating to damages[;]...[g]ood lawyering and careful instructions should keep the jury focused and on task even if liability and damages are tried together").

### 4. Due Process Considerations

Relying solely on the Supreme Court's decision in *Connecticut v. Doehr*, 501 U.S. 1, 111 S.Ct. 2105, 115 L.Ed.2d 1 (1991), defendants advance the novel argument that the Due Process Clause compels bifurcation in this case. In *Doehr*, the Supreme Court held that a Connecticut statute "authoriz[ing] prejudgment attachment of real estate without prior notice or hearing, without a showing of extraordinary circumstances, and without a requirement that the person seeking the attachment post a bond" violated the Due Process Clause. *Id.* at 4, 111 S.Ct. 2105. Defendants have not cited a single case applying *Doehr* in the context of a request for bifurcation of a personal injury case. This Court discerns no constitutional impediment under the Due Process Clause to trying together the issues of liability and damages.

In *Doehr*, the Supreme Court articulated a three-factor test for evaluating the procedures that a state must provide before depriving an individual of his property: "first, consideration of the private interest that will be affected by the...measure; second, an examination of the risk of erroneous deprivation through the procedures under attack and the probable value of additional or alternative safeguards; and third,...principal attention to the interest of the party seeking the prejudgment remedy, with, nonetheless, due regard for any ancillary interest the government may have in providing the procedure or forgoing the added burden of providing greater protections." *Id.* at 11, 111 S.Ct. 2105. In other words, defendants' argument rests on the premise that a non-bifurcated trial of this relatively straightforward personal injury case presents such a substantial risk of an erroneous outcome that it would be constitutionally foreclosed. The Due Process Clause does not compel such a result, particularly considering that courts across the country conduct non-bifurcated personal injury trials every day, and no evidence has been presented to conclude that the jury determinations of those matters are infected by impermissible considerations of sympathy.

In sum, I conclude that defendants have not shown that either the Due Process Clause or Fed. R. Civ. P. Rule 42(b) requires bifurcation of the trial in this matter.

## CONCLUSION

For the reasons discussed above, defendants' motion to exclude Timko's testimony **(Docket # 65)** is **GRANTED in PART and DENIED in PART**. Moody's motion for sanctions **(Docket # 68)** is **GRANTED**. Defendants' motion to bifurcate the trial **(Docket # 98)** is **DENIED**.

**IT IS SO ORDERED.**

**All Citations**

--- F.Supp.3d ----, 2017 WL 4173358

Footnotes

1 Moody's motion was initially filed as a cross-motion to defendants' motion for summary judgment. (Docket # 68). In its Decision and Order, the Court reserved decision on this issue. (*See* Docket # 90 at 27).

2 Operation Lifesaver is "a nonprofit public safety education and awareness organization dedicated to reducing collisions, fatalities and injuries at highway-rail crossings and trespassing on or near railroad tracks." Operation Lifesaver, *About Us*, https://oli.org/about-us (last accessed September 20, 2017).

3 With the Court's permission, defendants filed a sur-reply in which they argue that they should not be penalized for failing to check that Lewandowski had uploaded the correct data to the Vault and reiterate that they did not act culpably. (Docket # 85–1 at 3–5).

4 At oral argument, their counsel suggested that defendants should not be deemed responsible for their prior counsel's failure to perform a reasonable inquiry prior to submission of the answer. It is well-established, however, that represented parties may be subject to Rule 11 sanctions where they share responsibility for the violation. *See*, *e.g.*, *Braun ex rel. Advanced Battery Techs., Inc. v. Zhiguo Fu*, 2015 WL 4389893, *12 (S.D.N.Y. 2015) ("[u]nder Rule 11(c)(1), sanctions may be imposed not only against attorneys, but also against represented parties, where the party is responsible for the violation") (internal quotation omitted). Here, the fact that Lewandowski took steps to retrieve the event recorder data within hours of the accident evidences that defendants were aware of the importance of that information.

5 Rule 37(e)(2) "does not include a requirement that the court find prejudice to the party deprived of the information." Fed. R. Civ. P. 37(e)(2) advisory committee's note to 2015 amendment. As discussed below, the Court finds that defendants acted with an intent to deprive Moody of the event recorder data, and Rule 37(e)(2) thus applies. Accordingly, sanctions are warranted even in the absence of a finding of prejudice.

Reports of Cases

JUDGMENT OF THE COURT (Grand Chamber)

13 May 2014*

(Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Establishment on the territory of a Member State — Extent of that operator's obligations and of the data subject's rights — Charter of Fundamental Rights of the European Union — Articles 7 and 8)

In Case C-131/12,

REQUEST for a preliminary ruling under Article 267 TFEU from the Audiencia Nacional (Spain), made by decision of 27 February 2012, received at the Court on 9 March 2012, in the proceedings

**Google Spain SL,**

**Google Inc.**

v

**Agencia Española de Protección de Datos (AEPD),**

**Mario Costeja González,**

THE COURT (Grand Chamber),

composed of V. Skouris, President, K. Lenaerts, Vice-President, M. Ilešič (Rapporteur), L. Bay Larsen, T. von Danwitz, M. Safjan, Presidents of Chambers, J. Malenovský, E. Levits, A. Ó Caoimh, A. Arabadjiev, M. Berger, A. Prechal and E. Jarašiūnas Judges,

Advocate General: N. Jääskinen,

Registrar: M. Ferreira, Principal Administrator,

having regard to the written procedure and further to the hearing on 26 February 2013,

after considering the observations submitted on behalf of:

— Google Spain SL and Google Inc., by F. González Díaz, J. Baño Fos and B. Holles, abogados,

— Mr Costeja González, by J. Muñoz Rodríguez, abogado,

— the Spanish Government, by A. Rubio González, acting as Agent,

* Language of the case: Spanish.

— the Greek Government, by E.-M. Mamouna and K. Boskovits, acting as Agents,

— the Italian Government, by G. Palmieri, acting as Agent, and P. Gentili, avvocato dello Stato,

— the Austrian Government, by G. Kunnert and C. Pesendorfer, acting as Agents,

— the Polish Government, by B. Majczyna and M. Szpunar, acting as Agents,

— the European Commission, by I. Martínez del Peral and B. Martenczuk, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 25 June 2013,

gives the following

## Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 2(b) and (d), Article 4(1)(a) and (c), Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) and of Article 8 of the Charter of Fundamental Rights of the European Union ('the Charter').

2 The request has been made in proceedings between, on the one hand, Google Spain SL ('Google Spain') and Google Inc. and, on the other, the Agencia Española de Protección de Datos (Spanish Data Protection Agency; 'the AEPD') and Mr Costeja González concerning a decision by the AEPD upholding the complaint lodged by Mr Costeja González against those two companies and ordering Google Inc. to adopt the measures necessary to withdraw personal data relating to Mr Costeja González from its index and to prevent access to the data in the future.

### Legal context

*European Union law*

3 Directive 95/46 which, according to Article 1, has the object of protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, and of removing obstacles to the free flow of such data, states in recitals 2, 10, 18 to 20 and 25 in its preamble:

'(2) … data-processing systems are designed to serve man; … they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to … the well-being of individuals;

...

(10) … the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms [, signed in Rome on 4 November 1950,] and in the general principles of Community law; … for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

...

(18) … in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; … in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) … establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; … the legal form of such an establishment, whether simply [a] branch or a subsidiary with a legal personality, is not the determining factor in this respect; … when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) … the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; … in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

...

(25) … the principles of protection must be reflected, on the one hand, in the obligations imposed on persons … responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances'.

4 Article 2 of Directive 95/46 states that '[f]or the purposes of this Directive:

(a) "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

...

(d) "controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

...'

5 Article 3 of Directive 95/46, entitled 'Scope', states in paragraph 1:

'This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.'

6 Article 4 of Directive 95/46, entitled 'National law applicable', provides:

'1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1(c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.'

7 In Section I (entitled 'Principles relating to data quality') of Chapter II of Directive 95/46, Article 6 is worded as follows:

'1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.'

8 In Section II (entitled 'Criteria for making data processing legitimate') of Chapter II of Directive 95/46, Article 7 provides:

'Member States shall provide that personal data may be processed only if:

...

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests [or] fundamental rights and freedoms of the data subject which require protection under Article 1(1).'

9 Article 9 of Directive 95/46, entitled 'Processing of personal data and freedom of expression', provides:

'Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.'

10 Article 12 of Directive 95/46, entitled 'Rights of access', provides:

'Member States shall guarantee every data subject the right to obtain from the controller:

...

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

...'

11 Article 14 of Directive 95/46, entitled 'The data subject's right to object', provides:

'Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

...'

12 Article 28 of Directive 95/46, entitled 'Supervisory authority', is worded as follows:

'1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

...

3. Each authority shall in particular be endowed with:

— investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

— effective powers of intervention, such as, for example, that … of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing …

— …

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

…

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

…'

*Spanish law*

13 Directive 95/46 was transposed into Spanish Law by Organic Law No 15/1999 of 13 December 1999 on the protection of personal data (BOE No 298 of 14 December 1999, p. 43088).

## The dispute in the main proceedings and the questions referred for a preliminary ruling

14 On 5 March 2010, Mr Costeja González, a Spanish national resident in Spain, lodged with the AEPD a complaint against La Vanguardia Ediciones SL, which publishes a daily newspaper with a large circulation, in particular in Catalonia (Spain) ('La Vanguardia'), and against Google Spain and Google Inc. The complaint was based on the fact that, when an internet user entered Mr Costeja González's name in the search engine of the Google group ('Google Search'), he would obtain links to two pages of La Vanguardia's newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr Costeja González's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.

15 By that complaint, Mr Costeja González requested, first, that La Vanguardia be required either to remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data. Second, he requested that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results and no longer appeared in the links to La Vanguardia. Mr Costeja González stated in this context that the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant.

16 By decision of 30 July 2010, the AEPD rejected the complaint in so far as it related to La Vanguardia, taking the view that the publication by it of the information in question was legally justified as it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible.

17 On the other hand, the complaint was upheld in so far as it was directed against Google Spain and Google Inc. The AEPD considered in this regard that operators of search engines are subject to data protection legislation given that they carry out data processing for which they are responsible and act as intermediaries in the information society. The AEPD took the view that it has the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines when it considers that the locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense, and this would also encompass the mere wish of the person concerned that such data not be known to third parties. The AEPD considered that that obligation may be owed directly by operators of search engines, without it being necessary to erase the data or information from the website where they appear, including when retention of the information on that site is justified by a statutory provision.

18 Google Spain and Google Inc. brought separate actions against that decision before the Audiencia Nacional (National High Court). The Audiencia Nacional joined the actions.

19 That court states in the order for reference that the actions raise the question of what obligations are owed by operators of search engines to protect personal data of persons concerned who do not wish that certain information, which is published on third parties' websites and contains personal data relating to them that enable that information to be linked to them, be located, indexed and made available to internet users indefinitely. The answer to that question depends on the way in which Directive 95/46 must be interpreted in the context of these technologies, which appeared after the directive's publication.

20 In those circumstances, the Audiencia Nacional decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:

'1. With regard to the territorial application of Directive [95/46] and, consequently, of the Spanish data protection legislation:

(a) must it be considered that an "establishment", within the meaning of Article 4(1)(a) of Directive 95/46, exists when any one or more of the following circumstances arise:

— when the undertaking providing the search engine sets up in a Member State an office or subsidiary for the purpose of promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State,

or

— when the parent company designates a subsidiary located in that Member State as its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking,

or

— when the office or subsidiary established in a Member State forwards to the parent company, located outside the European Union, requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation of the right to data protection, even where such collaboration is engaged in voluntarily?

(b) Must Article 4(1)(c) of Directive 95/46 be interpreted as meaning that there is "use of equipment … situated on the territory of the said Member State":

— when a search engine uses crawlers or robots to locate and index information contained in web pages located on servers in that Member State,

or

— when it uses a domain name pertaining to a Member State and arranges for searches and the results thereof to be based on the language of that Member State?

(c) Is it possible to regard as a use of equipment, in the terms of Article 4(1)(c) of Directive 95/46, the temporary storage of the information indexed by internet search engines? If the answer to that question is affirmative, can it be considered that that connecting factor is present when the undertaking refuses to disclose the place where it stores those indexes, invoking reasons of competition?

(d) Regardless of the answers to the foregoing questions and particularly in the event that the Court … considers that the connecting factors referred to in Article 4 of [Directive 95/46] are not present:

must Directive 95/46 … be applied, in the light of Article 8 of the [Charter], in the Member State where the centre of gravity of the conflict is located and more effective protection of the rights of … Union citizens is possible?

2. As regards the activity of search engines as providers of content in relation to Directive 95/46 …:

(a) in relation to the activity of [Google Search], as a provider of content, consisting in locating information published or included on the net by third parties, indexing it automatically, storing it temporarily and finally making it available to internet users according to a particular order of preference, when that information contains personal data of third parties: must an activity like the one described be interpreted as falling within the concept of "processing of … data" used in Article 2(b) of Directive 95/46?

(b) If the answer to the foregoing question is affirmative, and once again in relation to an activity like the one described:

must Article 2(d) of Directive 95/46 be interpreted as meaning that the undertaking managing [Google Search] is to be regarded as the "controller" of the personal data contained in the web pages that it indexes?

(c) In the event that the answer to the foregoing question is affirmative:

may the [AEPD], protecting the rights embodied in [Article] 12(b) and [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, directly impose on [Google Search] a requirement that it withdraw from its indexes an item of information published by third parties, without addressing itself in advance or simultaneously to the owner of the web page on which that information is located?

(d) In the event that the answer to the foregoing question is affirmative:

would the obligation of search engines to protect those rights be excluded when the information that contains the personal data has been lawfully published by third parties and is kept on the web page from which it originates?

3. Regarding the scope of the right of erasure and/or the right to object, in relation to the "derecho al olvido" (the "right to be forgotten"), the following question is asked:

must it be considered that the rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for by [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, extend to enabling the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally, published on third parties' web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties?'

## Consideration of the questions referred

*Question 2(a) and (b), concerning the material scope of Directive 95/46*

21 By Question 2(a) and (b), which it is appropriate to examine first, the referring court asks, in essence, whether Article 2(b) of Directive 95/46 is to be interpreted as meaning that the activity of a search engine as a provider of content which consists in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of that provision when that information contains personal data. If the answer is in the affirmative, the referring court seeks to ascertain furthermore whether Article 2(d) of Directive 95/46 is to be interpreted as meaning that the operator of a search engine must be regarded as the 'controller' in respect of that processing of the personal data, within the meaning of that provision.

22 According to Google Spain and Google Inc., the activity of search engines cannot be regarded as processing of the data which appear on third parties' web pages displayed in the list of search results, given that search engines process all the information available on the internet without effecting a selection between personal data and other information. Furthermore, even if that activity must be classified as 'data processing', the operator of a search engine cannot be regarded as a 'controller' in respect of that processing since it has no knowledge of those data and does not exercise control over the data.

23 On the other hand, Mr Costeja González, the Spanish, Italian, Austrian and Polish Governments and the European Commission consider that that activity quite clearly involves 'data processing' within the meaning of Directive 95/46, which is distinct from the data processing by the publishers of websites and pursues different objectives from such processing. The operator of a search engine is the 'controller' in respect of the data processing carried out by it since it is the operator that determines the purposes and means of that processing.

24 In the Greek Government's submission, the activity in question constitutes such 'processing', but inasmuch as search engines serve merely as intermediaries, the undertakings which operate them cannot be regarded as 'controllers', except where they store data in an 'intermediate memory' or 'cache memory' for a period which exceeds that which is technically necessary.

25 Article 2(b) of Directive 95/46 defines 'processing of personal data' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction'.

26 As regards in particular the internet, the Court has already had occasion to state that the operation of loading personal data on an internet page must be considered to be such 'processing' within the meaning of Article 2(b) of Directive 95/46 (see Case C-101/01 *Lindqvist* EU:C:2003:596, paragraph 25).

27 So far as concerns the activity at issue in the main proceedings, it is not contested that the data found, indexed and stored by search engines and made available to their users include information relating to identified or identifiable natural persons and thus 'personal data' within the meaning of Article 2(a) of that directive.

28 Therefore, it must be found that, in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data.

29 Nor is the foregoing finding affected by the fact that those data have already been published on the internet and are not altered by the search engine.

30 The Court has already held that the operations referred to in Article 2(b) of Directive 95/46 must also be classified as such processing where they exclusively concern material that has already been published in unaltered form in the media. It has indeed observed in that regard that a general derogation from the application of Directive 95/46 in such a case would largely deprive the directive of its effect (see, to this effect, Case C-73/07 *Satakunnan Markkinapörssi and Satamedia* EU:C:2008:727, paragraphs 48 and 49).

31 Furthermore, it follows from the definition contained in Article 2(b) of Directive 95/46 that, whilst the alteration of personal data indeed constitutes processing within the meaning of the directive, the other operations which are mentioned there do not, on the other hand, in any way require that the personal data be altered.

32 As to the question whether the operator of a search engine must be regarded as the 'controller' in respect of the processing of personal data that is carried out by that engine in the context of an activity such as that at issue in the main proceedings, it should be recalled that Article 2(d) of Directive 95/46 defines 'controller' as 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data'.

33 It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing pursuant to Article 2(d).

34 Furthermore, it would be contrary not only to the clear wording of that provision but also to its objective — which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.

35 In this connection, it should be pointed out that the processing of personal data carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites, consisting in loading those data on an internet page.

36 Moreover, it is undisputed that that activity of search engines plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published.

37 Also, the organisation and aggregation of information published on the internet that are effected by search engines with the aim of facilitating their users' access to that information may, when users carry out their search on the basis of an individual's name, result in them obtaining through the list of results a structured overview of the information relating to that individual that can be found on the internet enabling them to establish a more or less detailed profile of the data subject.

38 Inasmuch as the activity of a search engine is therefore liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.

39 Finally, the fact that publishers of websites have the option of indicating to operators of search engines, by means in particular of exclusion protocols such as 'robot.txt' or codes such as 'noindex' or 'noarchive', that they wish specific information published on their site to be wholly or partially excluded from the search engines' automatic indexes does not mean that, if publishers of websites do not so indicate, the operator of a search engine is released from its responsibility for the processing of personal data that it carries out in the context of the engine's activity.

40 That fact does not alter the position that the purposes and means of that processing are determined by the operator of the search engine. Furthermore, even if that option for publishers of websites were to mean that they determine the means of that processing jointly with that operator, this finding would not remove any of the latter's responsibility as Article 2(d) of Directive 95/46 expressly provides that that determination may be made 'alone or jointly with others'.

41 It follows from all the foregoing considerations that the answer to Question 2(a) and (b) is that Article 2(b) and (d) of Directive 95/46 are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d).

*Question 1(a) to (d), concerning the territorial scope of Directive 95/46*

42 By Question 1(a) to (d), the referring court seeks to establish whether it is possible to apply the national legislation transposing Directive 95/46 in circumstances such as those at issue in the main proceedings.

43 In this respect, the referring court has established the following facts:

— Google Search is offered worldwide through the website 'www.google.com'. In numerous States, a local version adapted to the national language exists. The version of Google Search in Spanish is offered through the website 'www.google.es', which has been registered since 16 September 2003. Google Search is one of the most used search engines in Spain.

— Google Search is operated by Google Inc., which is the parent company of the Google Group and has its seat in the United States.

— Google Search indexes websites throughout the world, including websites located in Spain. The information indexed by its 'web crawlers' or robots, that is to say, computer programmes used to locate and sweep up the content of web pages methodically and automatically, is stored temporarily on servers whose State of location is unknown, that being kept secret for reasons of competition.

— Google Search does not merely give access to content hosted on the indexed websites, but takes advantage of that activity and includes, in return for payment, advertising associated with the internet users' search terms, for undertakings which wish to use that tool in order to offer their goods or services to the internet users.

— The Google group has recourse to its subsidiary Google Spain for promoting the sale of advertising space generated on the website 'www.google.com'. Google Spain, which was established on 3 September 2003 and possesses separate legal personality, has its seat in Madrid (Spain). Its activities are targeted essentially at undertakings based in Spain, acting as a commercial agent for the Google group in that Member State. Its objects are to promote, facilitate and effect the sale of on-line advertising products and services to third parties and the marketing of that advertising.

— Google Inc. designated Google Spain as the controller, in Spain, in respect of two filing systems registered by Google Inc. with the AEPD; those filing systems were intended to contain the personal data of the customers who had concluded contracts for advertising services with Google Inc.

44 Specifically, the main issues raised by the referring court concern the notion of 'establishment', within the meaning of Article 4(1)(a) of Directive 95/46, and of 'use of equipment situated on the territory of the said Member State', within the meaning of Article 4(1)(c).

Question 1(a)

45 By Question 1(a), the referring court asks, in essence, whether Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when one or more of the following three conditions are met:

— the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State, or

— the parent company designates a subsidiary located in that Member State as its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking, or

— the branch or subsidiary established in a Member State forwards to the parent company, located outside the European Union, requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation of the right to protection of personal data, even where such collaboration is engaged in voluntarily.

46 So far as concerns the first of those three conditions, the referring court states that Google Search is operated and managed by Google Inc. and that it has not been established that Google Spain carries out in Spain an activity directly linked to the indexing or storage of information or data contained on third parties' websites. Nevertheless, according to the referring court, the promotion and sale of advertising space, which Google Spain attends to in respect of Spain, constitutes the bulk of the Google group's commercial activity and may be regarded as closely linked to Google Search.

47 Mr Costeja González, the Spanish, Italian, Austrian and Polish Governments and the Commission submit that, in the light of the inextricable link between the activity of the search engine operated by Google Inc. and the activity of Google Spain, the latter must be regarded as an establishment of the former and the processing of personal data is carried out in context of the activities of that establishment. On the other hand, according to Google Spain, Google Inc. and the Greek Government, Article 4(1)(a) of Directive 95/46 is not applicable in the case of the first of the three conditions listed by the referring court.

48 In this regard, it is to be noted first of all that recital 19 in the preamble to Directive 95/46 states that 'establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements' and that 'the legal form of such an establishment, whether simply [a] branch or a subsidiary with a legal personality, is not the determining factor'.

49 It is not disputed that Google Spain engages in the effective and real exercise of activity through stable arrangements in Spain. As it moreover has separate legal personality, it constitutes a subsidiary of Google Inc. on Spanish territory and, therefore, an 'establishment' within the meaning of Article 4(1)(a) of Directive 95/46.

50 In order to satisfy the criterion laid down in that provision, it is also necessary that the processing of personal data by the controller be 'carried out in the context of the activities' of an establishment of the controller on the territory of a Member State.

51 Google Spain and Google Inc. dispute that this is the case since the processing of personal data at issue in the main proceedings is carried out exclusively by Google Inc., which operates Google Search without any intervention on the part of Google Spain; the latter's activity is limited to providing support to the Google group's advertising activity which is separate from its search engine service.

52 Nevertheless, as the Spanish Government and the Commission in particular have pointed out, Article 4(1)(a) of Directive 95/46 does not require the processing of personal data in question to be carried out 'by' the establishment concerned itself, but only that it be carried out 'in the context of the activities' of the establishment.

53 Furthermore, in the light of the objective of Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, those words cannot be interpreted restrictively (see, by analogy, Case C-324/09 *L'Oréal and Others* EU:C:2011:474, paragraphs 62 and 63).

54 It is to be noted in this context that it is clear in particular from recitals 18 to 20 in the preamble to Directive 95/46 and Article 4 thereof that the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope.

55 In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.

56 In such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.

57 As has been stated in paragraphs 26 to 28 of the present judgment, the very display of personal data on a search results page constitutes processing of such data. Since that display of results is accompanied, on the same page, by the display of advertising linked to the search terms, it is clear that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory.

58 That being so, it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure (see, by analogy, *L'Oréal and Others* EU:C:2011:474, paragraphs 62 and 63), in particular their right to privacy, with respect to the processing of personal data, a right to which the directive accords special importance as is confirmed in particular by Article 1(1) thereof and recitals 2 and 10 in its preamble (see, to this effect, Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 70; Case C-553/07 *Rijkeboer* EU:C:2009:293, paragraph 47; and Case C-473/12 *IPI* EU:C:2013:715, paragraph 28 and the case-law cited).

59 Since the first of the three conditions listed by the referring court suffices by itself for it to be concluded that an establishment such as Google Spain satisfies the criterion laid down in Article 4(1)(a) of Directive 95/46, it is unnecessary to examine the other two conditions.

60 It follows from the foregoing that the answer to Question 1(a) is that Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.

Question 1(b) to (d)

61 In view of the answer given to Question 1(a), there is no need to answer Question 1(b) to (d).

*Question 2(c) and (d), concerning the extent of the responsibility of the operator of a search engine under Directive 95/46*

62 By Question 2(c) and (d), the referring court asks, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information

relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

63 Google Spain and Google Inc. submit that, by virtue of the principle of proportionality, any request seeking the removal of information must be addressed to the publisher of the website concerned because it is he who takes the responsibility for making the information public, who is in a position to appraise the lawfulness of that publication and who has available to him the most effective and least restrictive means of making the information inaccessible. Furthermore, to require the operator of a search engine to withdraw information published on the internet from its indexes would take insufficient account of the fundamental rights of publishers of websites, of other internet users and of that operator itself.

64 According to the Austrian Government, a national supervisory authority may order such an operator to erase information published by third parties from its filing systems only if the data in question have been found previously to be unlawful or incorrect or if the data subject has made a successful objection to the publisher of the website on which that information was published.

65 Mr Costeja González, the Spanish, Italian and Polish Governments and the Commission submit that the national authority may directly order the operator of a search engine to withdraw from its indexes and intermediate memory information containing personal data that has been published by third parties, without having to approach beforehand or simultaneously the publisher of the web page on which that information appears. Furthermore, according to Mr Costeja González, the Spanish and Italian Governments and the Commission, the fact that the information has been published lawfully and that it still appears on the original web page has no effect on the obligations of that operator under Directive 95/46. On the other hand, according to the Polish Government that fact is such as to release the operator from its obligations.

66 First of all, it should be remembered that, as is apparent from Article 1 and recital 10 in the preamble, Directive 95/46 seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data (see, to this effect, *IPI* EU:C:2013:715, paragraph 28).

67 According to recital 25 in the preamble to Directive 95/46, the principles of protection laid down by the directive are reflected, on the one hand, in the obligations imposed on persons responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority and the circumstances under which processing can be carried out, and, on the other hand, in the rights conferred on individuals whose data are the subject of processing to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.

68 The Court has already held that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter (see, in particular, Case C-274/99 P *Connolly* v *Commission* EU:C:2001:127, paragraph 37, and *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 68).

69 Article 7 of the Charter guarantees the right to respect for private life, whilst Article 8 of the Charter expressly proclaims the right to the protection of personal data. Article 8(2) and (3) specify that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law, that everyone has the right of access to

data which have been collected concerning him or her and the right to have the data rectified, and that compliance with these rules is to be subject to control by an independent authority. Those requirements are implemented inter alia by Articles 6, 7, 12, 14 and 28 of Directive 95/46.

70 Article 12(b) of Directive 95/46 provides that Member States are to guarantee every data subject the right to obtain from the controller, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of Directive 95/46, in particular because of the incomplete or inaccurate nature of the data. As this final point relating to the case where certain requirements referred to in Article 6(1)(d) of Directive 95/46 are not observed is stated by way of example and is not exhaustive, it follows that non-compliant nature of the processing, which is capable of conferring upon the data subject the right guaranteed in Article 12(b) of the directive, may also arise from non-observance of the other conditions of lawfulness that are imposed by the directive upon the processing of personal data.

71 In this connection, it should be noted that, subject to the exceptions permitted under Article 13 of Directive 95/46, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive (see *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 65; Joined Cases C-468/10 and C-469/10 *ASNEF and FECEMD* EU:C:2011:777, paragraph 26; and Case C-342/12 *Worten* EU:C:2013:355, paragraph 33).

72 Under Article 6 of Directive 95/46 and without prejudice to specific provisions that the Member States may lay down in respect of processing for historical, statistical or scientific purposes, the controller has the task of ensuring that personal data are processed 'fairly and lawfully', that they are 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes', that they are 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed', that they are 'accurate and, where necessary, kept up to date' and, finally, that they are 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed'. In this context, the controller must take every reasonable step to ensure that data which do not meet the requirements of that provision are erased or rectified.

73 As regards legitimation, under Article 7 of Directive 95/46, of processing such as that at issue in the main proceedings carried out by the operator of a search engine, that processing is capable of being covered by the ground in Article 7(f).

74 This provision permits the processing of personal data where it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject — in particular his right to privacy with respect to the processing of personal data — which require protection under Article 1(1) of the directive. Application of Article 7(f) thus necessitates a balancing of the opposing rights and interests concerned, in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter (see *ASNEF and FECEMD*, EU:C:2011:777, paragraphs 38 and 40).

75 Whilst the question whether the processing complies with Articles 6 and 7(f) of Directive 95/46 may be determined in the context of a request as provided for in Article 12(b) of the directive, the data subject may, in addition, rely in certain conditions on the right to object laid down in subparagraph (a) of the first paragraph of Article 14 of the directive.

76 Under subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, Member States are to grant the data subject the right, at least in the cases referred to in Article 7(e) and (f) of the directive, to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. The

balancing to be carried out under subparagraph (a) of the first paragraph of Article 14 thus enables account to be taken in a more specific manner of all the circumstances surrounding the data subject's particular situation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.

77 Requests under Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 may be addressed by the data subject directly to the controller who must then duly examine their merits and, as the case may be, end processing of the data in question. Where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders the controller to take specific measures accordingly.

78 In this connection, it is to be noted that it is clear from Article 28(3) and (4) of Directive 95/46 that each supervisory authority is to hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data and that it has investigative powers and effective powers of intervention enabling it to order in particular the blocking, erasure or destruction of data or to impose a temporary or definitive ban on such processing.

79 It is in the light of those considerations that it is necessary to interpret and apply the provisions of Directive 95/46 governing the data subject's rights when he lodges with the supervisory authority or judicial authority a request such as that at issue in the main proceedings.

80 It must be pointed out at the outset that, as has been found in paragraphs 36 to 38 of the present judgment, processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (see, to this effect, Joined Cases C-509/09 and C-161/10 *eDate Advertising and Others* EU:C:2011:685, paragraph 45).

81 In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing. However, inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

82 Following the appraisal of the conditions for the application of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 which is to be carried out when a request such as that at issue in the main proceedings is lodged with it, the supervisory authority or judicial authority may order the operator of the search engine to remove from the list of results displayed following a search made on the basis of a person's name links to web pages published by third parties containing

information relating to that person, without an order to that effect presupposing the previous or simultaneous removal of that name and information — of the publisher's own accord or following an order of one of those authorities — from the web page on which they were published.

83 As has been established in paragraphs 35 to 38 of the present judgment, inasmuch as the data processing carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites and affects the data subject's fundamental rights additionally, the operator of the search engine as the controller in respect of that processing must ensure, within the framework of its responsibilities, powers and capabilities, that that processing meets the requirements of Directive 95/46, in order that the guarantees laid down by the directive may have full effect.

84 Given the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites.

85 Furthermore, the processing by the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out 'solely for journalistic purposes' and thus benefit, by virtue of Article 9 of Directive 95/46, from derogations from the requirements laid down by the directive, whereas that does not appear to be so in the case of the processing carried out by the operator of a search engine. It cannot therefore be ruled out that in certain circumstances the data subject is capable of exercising the rights referred to in Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 against that operator but not against the publisher of the web page.

86 Finally, it must be stated that not only does the ground, under Article 7 of Directive 95/46, justifying the publication of a piece of personal data on a website not necessarily coincide with that which is applicable to the activity of search engines, but also, even where that is the case, the outcome of the weighing of the interests at issue to be carried out under Article 7(f) and subparagraph (a) of the first paragraph of Article 14 of the directive may differ according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of the web page is at issue, given that, first, the legitimate interests justifying the processing may be different and, second, the consequences of the processing for the data subject, and in particular for his private life, are not necessarily the same.

87 Indeed, since the inclusion in the list of results, displayed following a search made on the basis of a person's name, of a web page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page.

88 In the light of all the foregoing considerations, the answer to Question 2(c) and (d) is that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

*Question 3, concerning the scope of the data subject's rights guaranteed by Directive 95/46*

89 By Question 3, the referring court asks, in essence, whether Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as enabling the data subject to require the operator of a search engine to remove from the list of results displayed following a search made on the basis of his name links to web pages published lawfully by third parties and containing true information relating to him, on the ground that that information may be prejudicial to him or that he wishes it to be 'forgotten' after a certain time.

90 Google Spain, Google Inc., the Greek, Austrian and Polish Governments and the Commission consider that this question should be answered in the negative. Google Spain, Google Inc., the Polish Government and the Commission submit in this regard that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 confer rights upon data subjects only if the processing in question is incompatible with the directive or on compelling legitimate grounds relating to their particular situation, and not merely because they consider that that processing may be prejudicial to them or they wish that the data being processed sink into oblivion. The Greek and Austrian Governments submit that the data subject must approach the publisher of the website concerned.

91 According to Mr Costeja González and the Spanish and Italian Governments, the data subject may oppose the indexing by a search engine of personal data relating to him where their dissemination through the search engine is prejudicial to him and his fundamental rights to the protection of those data and to privacy — which encompass the 'right to be forgotten' — override the legitimate interests of the operator of the search engine and the general interest in freedom of information.

92 As regards Article 12(b) of Directive 95/46, the application of which is subject to the condition that the processing of personal data be incompatible with the directive, it should be recalled that, as has been noted in paragraph 72 of the present judgment, such incompatibility may result not only from the fact that such data are inaccurate but, in particular, also from the fact that they are inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific purposes.

93 It follows from those requirements, laid down in Article 6(1)(c) to (e) of Directive 95/46, that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.

94 Therefore, if it is found, following a request by the data subject pursuant to Article 12(b) of Directive 95/46, that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased.

95 So far as concerns requests as provided for by Article 12(b) of Directive 95/46 founded on alleged non-compliance with the conditions laid down in Article 7(f) of the directive and requests under subparagraph (a) of the first paragraph of Article 14 of the directive, it must be pointed out that in each case the processing of personal data must be authorised under Article 7 for the entire period during which it is carried out.

96 In the light of the foregoing, when appraising such requests made in order to oppose processing such as that at issue in the main proceedings, it should in particular be examined whether the data subject has a right that the information relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name. In this connection, it must be pointed out that it is not necessary in order to find such a right that the inclusion of the information in question in the list of results causes prejudice to the data subject.

97 As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results, it should be held, as follows in particular from paragraph 81 of the present judgment, that those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.

98 As regards a situation such as that at issue in the main proceedings, which concerns the display, in the list of results that the internet user obtains by making a search by means of Google Search on the basis of the data subject's name, of links to pages of the on-line archives of a daily newspaper that contain announcements mentioning the data subject's name and relating to a real-estate auction connected with attachment proceedings for the recovery of social security debts, it should be held that, having regard to the sensitivity for the data subject's private life of the information contained in those announcements and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that that information should no longer be linked to his name by means of such a list. Accordingly, since in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that information, a matter which is, however, for the referring court to establish, the data subject may, by virtue of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, require those links to be removed from the list of results.

99 It follows from the foregoing considerations that the answer to Question 3 is that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.

## Costs

100 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1. **Article 2(b) and (d) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d).**

2. **Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.**

3. **Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.**

4. **Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.**

[Signatures]

United States Code Annotated
Federal Rules of Civil Procedure for the United States District Courts (Refs & Annos)
Title V. Disclosures and Discovery (Refs & Annos)

Federal Rules of Civil Procedure Rule 37

Rule 37. Failure to Make Disclosures or to Cooperate in Discovery; Sanctions

Currentness

**(a) Motion for an Order Compelling Disclosure or Discovery.**

**(1)** ***In General.*** On notice to other parties and all affected persons, a party may move for an order compelling disclosure or discovery. The motion must include a certification that the movant has in good faith conferred or attempted to confer with the person or party failing to make disclosure or discovery in an effort to obtain it without court action.

**(2)** ***Appropriate Court.*** A motion for an order to a party must be made in the court where the action is pending. A motion for an order to a nonparty must be made in the court where the discovery is or will be taken.

**(3)** ***Specific Motions.***

**(A)** *To Compel Disclosure.* If a party fails to make a disclosure required by Rule 26(a), any other party may move to compel disclosure and for appropriate sanctions.

**(B)** *To Compel a Discovery Response.* A party seeking discovery may move for an order compelling an answer, designation, production, or inspection. This motion may be made if:

**(i)** a deponent fails to answer a question asked under Rule 30 or 31;

**(ii)** a corporation or other entity fails to make a designation under Rule 30(b)(6) or 31(a)(4);

**(iii)** a party fails to answer an interrogatory submitted under Rule 33; or

**(iv)** a party fails to produce documents or fails to respond that inspection will be permitted -- or fails to permit inspection -- as requested under Rule 34.

**(C)** *Related to a Deposition.* When taking an oral deposition, the party asking a question may complete or adjourn the examination before moving for an order.

**(4)** ***Evasive or Incomplete Disclosure, Answer, or Response.*** For purposes of this subdivision (a), an evasive or incomplete disclosure, answer, or response must be treated as a failure to disclose, answer, or respond.

**(5)** ***Payment of Expenses; Protective Orders.***

**(A)** *If the Motion Is Granted (or Disclosure or Discovery Is Provided After Filing).* If the motion is granted--or if the disclosure or requested discovery is provided after the motion was filed--the court must, after giving an opportunity to be heard, require the party or deponent whose conduct necessitated the motion, the party or attorney advising that conduct, or both to pay the movant's reasonable expenses incurred in making the motion, including attorney's fees. But the court must not order this payment if:

**(i)** the movant filed the motion before attempting in good faith to obtain the disclosure or discovery without court action;

**(ii)** the opposing party's nondisclosure, response, or objection was substantially justified; or

**(iii)** other circumstances make an award of expenses unjust.

**(B)** *If the Motion Is Denied.* If the motion is denied, the court may issue any protective order authorized under Rule 26(c) and must, after giving an opportunity to be heard, require the movant, the attorney filing the motion, or both to pay the party or deponent who opposed the motion its reasonable expenses incurred in opposing the motion, including attorney's fees. But the court must not order this payment if the motion was substantially justified or other circumstances make an award of expenses unjust.

**(C)** *If the Motion Is Granted in Part and Denied in Part.* If the motion is granted in part and denied in part, the court may issue any protective order authorized under Rule 26(c) and may, after giving an opportunity to be heard, apportion the reasonable expenses for the motion.

**(b) Failure to Comply with a Court Order.**

**(1)** ***Sanctions Sought in the District Where the Deposition Is Taken.*** If the court where the discovery is taken orders a deponent to be sworn or to answer a question and the deponent fails to obey, the failure may be treated as contempt of court. If a deposition-related motion is transferred to the court where the action is pending, and that court orders a deponent to be sworn or to answer a question and the deponent fails to obey, the failure may be treated as contempt of either the court where the discovery is taken or the court where the action is pending.

**(2)** ***Sanctions Sought in the District Where the Action Is Pending.***

**(A)** *For Not Obeying a Discovery Order.* If a party or a party's officer, director, or managing agent--or a witness designated under Rule 30(b)(6) or 31(a)(4)--fails to obey an order to provide or permit discovery, including an order

under Rule 26(f), 35, or 37(a), the court where the action is pending may issue further just orders. They may include the following:

**(i)** directing that the matters embraced in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims;

**(ii)** prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence;

**(iii)** striking pleadings in whole or in part;

**(iv)** staying further proceedings until the order is obeyed;

**(v)** dismissing the action or proceeding in whole or in part;

**(vi)** rendering a default judgment against the disobedient party; or

**(vii)** treating as contempt of court the failure to obey any order except an order to submit to a physical or mental examination.

**(B)** *For Not Producing a Person for Examination.* If a party fails to comply with an order under Rule 35(a) requiring it to produce another person for examination, the court may issue any of the orders listed in Rule 37(b)(2)(A)(i)-(vi), unless the disobedient party shows that it cannot produce the other person.

**(C)** *Payment of Expenses.* Instead of or in addition to the orders above, the court must order the disobedient party, the attorney advising that party, or both to pay the reasonable expenses, including attorney's fees, caused by the failure, unless the failure was substantially justified or other circumstances make an award of expenses unjust.

**(c) Failure to Disclose, to Supplement an Earlier Response, or to Admit.**

**(1)** ***Failure to Disclose or Supplement.*** If a party fails to provide information or identify a witness as required by Rule 26(a) or (e), the party is not allowed to use that information or witness to supply evidence on a motion, at a hearing, or at a trial, unless the failure was substantially justified or is harmless. In addition to or instead of this sanction, the court, on motion and after giving an opportunity to be heard:

**(A)** may order payment of the reasonable expenses, including attorney's fees, caused by the failure;

**(B)** may inform the jury of the party's failure; and

**(C)** may impose other appropriate sanctions, including any of the orders listed in Rule 37(b)(2)(A)(i)-(vi).

**(2)** ***Failure to Admit.*** If a party fails to admit what is requested under Rule 36 and if the requesting party later proves a document to be genuine or the matter true, the requesting party may move that the party who failed to admit pay the reasonable expenses, including attorney's fees, incurred in making that proof. The court must so order unless:

**(A)** the request was held objectionable under Rule 36(a);

**(B)** the admission sought was of no substantial importance;

**(C)** the party failing to admit had a reasonable ground to believe that it might prevail on the matter; or

**(D)** there was other good reason for the failure to admit.

**(d) Party's Failure to Attend Its Own Deposition, Serve Answers to Interrogatories, or Respond to a Request for Inspection.**

**(1)** ***In General.***

**(A)** *Motion; Grounds for Sanctions.* The court where the action is pending may, on motion, order sanctions if:

**(i)** a party or a party's officer, director, or managing agent--or a person designated under Rule 30(b)(6) or 31(a)(4)--fails, after being served with proper notice, to appear for that person's deposition; or

**(ii)** a party, after being properly served with interrogatories under Rule 33 or a request for inspection under Rule 34, fails to serve its answers, objections, or written response.

**(B)** *Certification.* A motion for sanctions for failing to answer or respond must include a certification that the movant has in good faith conferred or attempted to confer with the party failing to act in an effort to obtain the answer or response without court action.

**(2)** ***Unacceptable Excuse for Failing to Act.*** A failure described in Rule 37(d)(1)(A) is not excused on the ground that the discovery sought was objectionable, unless the party failing to act has a pending motion for a protective order under Rule 26(c).

**(3)** ***Types of Sanctions.*** Sanctions may include any of the orders listed in Rule 37(b)(2)(A)(i)-(vi). Instead of or in addition to these sanctions, the court must require the party failing to act, the attorney advising that party, or both to pay the reasonable expenses, including attorney's fees, caused by the failure, unless the failure was substantially justified or other circumstances make an award of expenses unjust.

**(e) Failure to Preserve Electronically Stored Information.** If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

**(1)** upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

**(2)** only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:

**(A)** presume that the lost information was unfavorable to the party;

**(B)** instruct the jury that it may or must presume the information was unfavorable to the party; or

**(C)** dismiss the action or enter a default judgment.

**(f) Failure to Participate in Framing a Discovery Plan.** If a party or its attorney fails to participate in good faith in developing and submitting a proposed discovery plan as required by Rule 26(f), the court may, after giving an opportunity to be heard, require that party or attorney to pay to any other party the reasonable expenses, including attorney's fees, caused by the failure.

**CREDIT(S)**

(Amended December 29, 1948, effective October 20, 1949; March 30, 1970, effective July 1, 1970; April 29, 1980, effective August 1, 1980; amended by Pub.L. 96-481, Title II, § 205(a), October 21, 1980, 94 Stat. 2330, effective October 1, 1981; amended March 2, 1987, effective August 1, 1987; April 22, 1993, effective December 1, 1993; April 17, 2000, effective December 1, 2000; April 12, 2006, effective December 1, 2006; April 30, 2007, effective December 1, 2007; April 16, 2013, effective December 1, 2013; April 29, 2015, effective December 1, 2015.)

**ADVISORY COMMITTEE NOTES**

**1937 Adoption**

The provisions of this rule authorizing orders establishing facts or excluding evidence or striking pleadings, or authorizing judgments of dismissal or default, for refusal to answer questions or permit inspection or otherwise make discovery, are in accord with *Hammond Packing Co. v. Arkansas,* 1909, 29 S.Ct. 370, 212 U.S. 322, 53 L.Ed. 530, 15 Ann.Cas. 645, which distinguishes between the justifiable use of such measures as a means of compelling the production of evidence, and their unjustifiable use, as in *Hovey v. Elliott,* 1897, 17 S.Ct. 841, 167 U.S. 409, 42 L.Ed. 215, for the mere purpose of punishing for contempt.

**1948 Amendment**

The amendment effective October 1949, substituted the reference to "Title 28, U.S.C., § 1783" in subdivision (e) for the reference to "the Act of July 3, 1926, c. 762, § 1 (44 Stat. 835), U.S.C., Title 28, § 711."

**1970 Amendment**

Rule 37 provides generally for sanctions against parties or persons unjustifiably resisting discovery. Experience has brought to light a number of defects in the language of the rule as well as instances in which it is not serving the purposes for which it was designed. See Rosenberg, *Sanctions to Effectuate Pretrial Discovery,* 58 Col.L.Rev. 480 (1958). In addition, changes being made in other discovery rules require conforming amendments to Rule 37.

Rule 37 sometimes refers to a "failure" to afford discovery and at other times to a "refusal" to do so. Taking note of this dual terminology, courts have imported into "refusal" a requirement of "wilfullness." See *Roth v. Paramount Pictures Corp.,* 8 F.R.D. 31 (W.D.Pa.1948); *Campbell v. Johnson,* 101 F.Supp. 705, 707 (S.D.N.Y.1951). In *Societe Internationale v. Rogers,* 357 U.S. 197 (1958), the Supreme Court concluded that the rather random use of these two terms in Rule 37 showed no design to use them with consistently distinctive meanings, that "refused" in Rule 37(b)(2) meant simply a failure to comply, and that wilfullness was relevant only to the selection of sanctions, if any, to be imposed. Nevertheless, after the decision in *Societe*, the court in *Hinson v. Michigan Mutual Liability Co.,* 275 F.2d 537 (5th Cir. 1960) once again ruled that "refusal" required wilfullness. Substitution of "failure" for "refusal" throughout Rule 37 should eliminate this confusion and bring the rule into harmony with the *Societe Internationale* decision. See Rosenberg, *supra*, 58 Col.L.Rev. 480, 489-490 (1958).

**Subdivision (a).** Rule 37(a) provides relief to a party seeking discovery against one who, with or without stated objections, fails to afford the discovery sought. It has always fully served this function in relation to depositions, but the amendments being made to Rules 33 and 34 give Rule 37(a) added scope and importance. Under existing Rule 33, a party objecting to interrogatories must make a motion for court hearing on his objections. The changes now made in Rules 33 and 37(a) make it clear that the interrogating party must move to compel answers, and the motion is provided for in Rule 37(a). Existing Rule 34, since it requires a court order prior to production of documents or things or permission to enter on land, has no relation to Rule 37(a). Amendments of Rules 34 and 37(a) create a procedure similar to that provided for Rule 33.

**Subdivision (a)(1).** This is a new provision making clear to which court a party may apply for an order compelling discovery. Existing Rule 37(a) refers only to the court in which the deposition is being taken; nevertheless, it has been held that the court where the action is pending has "inherent power" to compel a party deponent to answer. *Lincoln Laboratories, Inc. v. Savage Laboratories, Inc.,* 27 F.R.D. 476 (D.Del.1961). In relation to Rule 33 interrogatories and Rule 34 requests for inspection, the court where the action is pending is the appropriate enforcing tribunal. The new provision eliminates the need to resort to inherent power by spelling out the respective roles of the court where the action is pending and the court where the deposition is taken. In some instances, two courts are available to a party seeking to compel answers from a party deponent. The party seeking discovery may choose the court to which he will apply, but the court has power to remit the party to the other court as a more appropriate forum.

**Subdivision (a)(2).** This subdivision contains the substance of existing provisions of Rule 37(a) authorizing motions to compel answers to questions put at depositions and to interrogatories. New provisions authorize motions for orders compelling designation under Rules 30(b)(6) and 31(a) and compelling inspection in accordance with a request made under Rule 34. If the court denies a motion, in whole or part, it may accompany the denial with issuance of a protective order. Compare the converse provision in Rule 26(c).

**Subdivision (a)(3).** This new provision makes clear that an evasive or incomplete answer is to be considered, for purposes of subdivision (a), a failure to answer. The courts have consistently held that they have the power to compel adequate answers. *E.g., Cone Mills Corp. v. Joseph Bancroft & Sons Co.,* 33 F.R.D. 318 (D.Del.1963). This power is recognized and incorporated into the rule.

**Subdivision (a)(4).** This subdivision amends the provisions for award of expenses, including reasonable attorney's fees, to the prevailing party or person when a motion is made for an order compelling discovery. At present, an award of

expenses is made only if the losing party or person is found to have acted without substantial justification. The change requires that expenses be awarded unless the conduct of the losing party or person is found to have been substantially justified. The test of "substantial justification" remains, but the change in language is intended to encourage judges to be more alert to abuses occurring in the discovery process.

On many occasions, to be sure, the dispute over discovery between the parties is genuine, though ultimately resolved one way or the other by the court. In such cases, the losing party is substantially justified in carrying the matter to court. But the rules should deter the abuse implicit in carrying or forcing a discovery dispute to court when no genuine dispute exists. And the potential or actual imposition of expenses is virtually the sole formal sanction in the rules to deter a party from pressing to a court hearing frivolous requests for or objections to discovery.

The present provision of Rule 37(a) that the court shall require payment if it finds that the defeated party acted without "substantial justification" may appear adequate, but in fact it has been little used. Only a handful of reported cases include an award of expenses, and the Columbia Survey found that in only one instance out of about 50 motions decided under Rule 37(a) did the court award expenses. It appears that the courts do not utilize the most important available sanction to deter abusive resort to the judiciary.

The proposed change provides in effect that expenses should ordinarily be awarded unless a court finds that the losing party acted justifiably in carrying his point to court. At the same time, a necessary flexibility is maintained, since the court retains the power to find that other circumstances make an award of expenses unjust--as where the prevailing party also acted unjustifiably. The amendment does not significantly narrow the discretion of the court, but rather presses the court to address itself to abusive practices. The present provision that expenses may be imposed upon either the party or his attorney or both is unchanged. But it is not contemplated that expenses will be imposed upon the attorney merely because the party is indigent.

**Subdivision (b).** This subdivision deals with sanctions for failure to comply with a court order. The present captions for subsections (1) and (2) entitled, "Contempt" and "Other Consequences," respectively, are confusing. One of the consequences listed in (2) is the arrest of the party, representing the exercise of the contempt power. The contents of the subsections show that the first authorizes the sanction of contempt (and no other) by the court in which the deposition is taken, whereas the second subsection authorizes a variety of sanctions, including contempt, which may be imposed by the court in which the action is pending. The captions of the subsections are changed to reflect their contents.

The scope of Rule 37(b)(2) is broadened by extending it to include any order "to provide or permit discovery," including orders issued under Rules 37(a) and 35. Various rules authorize orders for discovery--*e.g.,* Rule 35(b)(1), Rule 26(c) as revised, Rule 37(d). See Rosenberg, *supra*, 58 Col.L.Rev. 480, 484-486. Rule 37(b)(2) should provide comprehensively for enforcement of all these orders. *Cf. Societe Internationale v. Rogers,* 357 U.S. 197, 207 (1958). On the other hand, the reference to Rule 34 is deleted to conform to the changed procedure in that rule.

A new subsection (E) provides that sanctions which have been available against a party for failure to comply with an order under Rule 35(a) to submit to examination will now be available against him for his failure to comply with a Rule 35(a) order to produce a third person for examination, unless he shows that he is unable to produce the person. In this context, "unable" means in effect "unable in good faith." See *Societe Internationale v. Rogers,* 357 U.S. 197 (1958).

Subdivision (b)(2) is amplified to provide for payment of reasonable expenses caused by the failure to obey the order. Although Rules 37(b)(2) and 37(d) have been silent as to award of expenses, courts have nevertheless ordered them on occasion. *E.g., United Sheeplined Clothing Co. v. Arctic Fur Cap Corp.,* 165 F.Supp. 193 (S.D.N.Y.1958); *Austin Theatre, Inc. v. Warner Bros. Pictures, Inc.,* 22 F.R.D. 302 (S.D.N.Y.1958). The provision places the burden on the disobedient party to avoid expenses by showing that his failure is justified or that special circumstances make an award

of expenses unjust. Allocating the burden in this way conforms to the changed provisions as to expenses in Rule 37(a), and is particularly appropriate when a court order is disobeyed.

An added reference to directors of a party is similar to a change made in subdivision (d) and is explained in the note to that subdivision. The added reference to persons designated by a party under Rules 30(b)(6) or 31(a) to testify on behalf of the party carries out the new procedure in those rules for taking a deposition of a corporation or other organization.

**Subdivision (c).** Rule 37(c) provides a sanction for the enforcement of Rule 36 dealing with requests for admission. Rule 36 provides the mechanism whereby a party may obtain from another party in appropriate instances either (1) an admission, or (2) a sworn and specific denial or (3) a sworn statement "setting forth in detail the reasons why he cannot truthfully admit or deny." If the party obtains the second or third of these responses, in proper form, Rule 36 does not provide for a pretrial hearing on whether the response is warranted by the evidence thus far accumulated. Instead, Rule 37(c) is intended to provide posttrial relief in the form of a requirement that the party improperly refusing the admission pay the expenses of the other side in making the necessary proof at trial.

Rule 37(c), as now written, addresses itself in terms only to the sworn denial and is silent with respect to the statement of reasons for an inability to admit or deny. There is no apparent basis for this distinction, since the sanction provided in Rule 37(c) should deter all unjustified failures to admit. This omission in the rule has caused confused and diverse treatment in the courts. One court has held that if a party give inadequate reasons, he should be treated before trial as having denied the request, so that Rule 37(c) may apply. *Bertha Bldg. Corp. v. National Theatres Corp.,* 15 F.R.D. 339 (E.D.N.Y.1954). Another has held that the party should be treated as having admitted the request. *Heng Hsin Co. v. Stern, Morgenthau & Co.,* 20 Fed.Rules Serv. 36a.52, Case 1 (S.D.N.Y. Dec. 10, 1954). Still another has ordered a new response, without indicating what the outcome should be if the new response were inadequate. *United States Plywood Corp. v. Hudson Lumber Co.,* 127 F.Supp. 489, 497-498 (S.D.N.Y.1954). See generally Finman, *The Request for Admissions in Federal Civil Procedure,* 71 Yale L.J. 371, 426-430 (1962). The amendment eliminates this defect in Rule 37(c) by bringing within its scope all failures to admit.

Additional provisions in Rule 37(c) protect a party from having to pay expenses if the request for admission was held objectionable under Rule 36(a) or if the party failing to admit had reasonable ground to believe that he might prevail on the matter. The latter provision emphasizes that the true test under Rule 37(c) is not whether a party prevailed at trial but whether he acted reasonably in believing that he might prevail.

**Subdivision (d).** The scope of subdivision (d) is broadened to include responses to requests for inspection under Rule 34, thereby conforming to the new procedures of Rule 34.

Two related changes are made in subdivision (d): the permissible sanctions are broadened to include such orders "as are just"; and the requirement that the failure to appear or respond be "wilful" is eliminated. Although Rule 37(d) in terms provides for only three sanctions, all rather severe, the courts have interpreted it as permitting softer sanctions than those which it sets forth. E.g., *Gill v. Stolow,* 240 F.2d 669 (2d Cir.1957); *Saltzman v. Birrell,* 156 F.Supp. 538 (S.D.N.Y.1957); 2A Barron & Holtzoff, *Federal Practice and Procedure* 554-557 (Wright ed. 1961). The rule is changed to provide the greater flexibility as to sanctions which the cases show is needed.

The resulting flexibility as to sanctions eliminates any need to retain the requirement that the failure to appear or respond be "wilful." The concept of "wilful failure" is at best subtle and difficult, and the cases do not supply a bright line. Many courts have imposed sanctions without referring to wilfullness. E.g., *Milewski v. Schneider Transportation Co.,* 238 F.2d 397 (6th Cir.1956); *Dictograph Products, Inc. v. Kentworth Corp.,* 7 F.R.D. 543 (W.D.Ky.1947). In addition, in view of the possibility of light sanctions, even a negligent failure should come within Rule 37(d). If default is caused by counsel's ignorance of Federal practice, cf. *Dunn v. Pa. R.R.,* 96 F.Supp. 597 (N.D.Ohio 1951), or by his preoccupation with another aspect of the case, *cf. Maurer-Neuer, Inc. v. United Packinghouse Workers,* 26 F.R.D. 139 (D.Kans.1960),

dismissal of the action and default judgment are not justified, but the imposition of expenses and fees may well be. "Wilfullness" continues to play a role, along with various other factors, in the choice of sanctions. Thus, the scheme conforms to Rule 37(b) as construed by the Supreme Court in *Societe Internationale v. Rogers,* 357 U.S. 197, 208 (1958).

A provision is added to make clear that a party may not properly remain completely silent even when he regards a notice to take his deposition or a set of interrogatories or requests to inspect as improper and objectionable. If he desires not to appear or not to respond, he must apply for a protective order. The cases are divided on whether a protective order must be sought. Compare *Collins v. Wayland,* 139 F.2d 677 (9th Cir. 1944), *cert. den.* 322 U.S. 744; *Bourgeois v. El Paso Natural Gas Co.,* 20 F.R.D. 358 (S.D.N.Y.1957); *Loosley v. Stone,* 15 F.R.D. 373 (S.D.Ill.1954), with *Scarlatos v. Kulukundis,* 21 F.R.D. 185 (S.D.N.Y.1957); *Ross v. True Temper Corp.,* 11 F.R.D. 307 (N.D.Ohio 1951). Compare also Rosenberg, *supra*, 58 Col.L.Rev. 480, 496 (1958) with 2A Barron & Holtzoff, *Federal Practice and Procedure* 530-531 (Wright ed. 1961). The party from whom discovery is sought is afforded, through Rule 26(c), a fair and effective procedure whereby he can challenge the request made. At the same time, the total noncompliance with which Rule 37(d) is concerned may impose severe inconvenience or hardship on the discovering party and substantially delay the discovery process. Cf. 2B Barron & Holtzoff, *Federal Practice and Procedure* 306-307 (Wright ed. 1961) (response to a subpoena).

The failure of an officer or managing agent of a party to make discovery as required by present Rule 37(d) is treated as the failure of the party. The rule as revised provides similar treatment for a director of a party. There is slight warrant for the present distinction between officers and managing agents on the one hand and directors on the other. Although the legal power over a director to compel his making discovery may not be as great as over officers or managing agents, *Campbell v. General Motors Corp.,* 13 F.R.D. 331 (S.D.N.Y.1952), the practical differences are negligible. That a director's interests are normally aligned with those of his corporation is shown by the provisions of old Rule 26(d)(2), transferred to 32(a)(2) (deposition of director of party may be used at trial by an adverse party for any purpose) and of Rule 43(b) (director of party may be treated at trial as a hostile witness on direct examination by any adverse party). Moreover, in those rare instances when a corporation is unable through good faith efforts to compel a director to make discovery, it is unlikely that the court will impose sanctions. Cf. *Societe Internationale v. Rogers,* 357 U.S. 197 (1958).

**Subdivision (e).** The change in the caption conforms to the language of 28 U.S.C. § 1783, as amended in 1964.

**Subdivision (f).** Until recently, costs of a civil action could be awarded against the United States only when expressly provided by Act of Congress, and such provision was rarely made. See H.R.Rep.No. 1535, 89th Cong., 2d Sess., 2-3 (1966). To avoid any conflict with this doctrine, Rule 37(f) has provided that expenses and attorney's fees may not be imposed upon the United States under Rule 37. See 2A Barron & Holtzoff, *Federal Practice and Procedure* 857 (Wright ed. 1961).

A major change in the law was made in 1966, 80 Stat. 308, 28 U.S.C. § 2412 (1966), whereby a judgment for costs may ordinarily be awarded to the prevailing party in any civil action brought by or against the United States. Costs are not to include the fees and expenses of attorneys. In light of this legislative development, Rule 37(f) is amended to permit the award of expenses and fees against the United States under Rule 37, but only to the extent permitted by statute. The amendment brings Rule 37(f) into line with present and future statutory provisions.

**1980 Amendment**

**Subdivision (b)(2).** New Rule 26(f) provides that if a discovery conference is held, at its close the court shall enter an order respecting the subsequent conduct of discovery. The amendment provides that the sanctions available for violation of other court orders respecting discovery are available for violation of the discovery conference order.

**Subdivision (e).** Subdivision (e) is stricken. Title 28, U.S.C. § 1783 no longer refers to sanctions. The subdivision otherwise duplicates Rule 45(e)(2).

**Subdivision (g).** New Rule 26(f) imposes a duty on parties to participate in good faith in the framing of a discovery plan by agreement upon the request of any party. This subdivision authorizes the court to award to parties who participate in good faith in an attempt to frame a discovery plan the expenses incurred in the attempt if any party or his attorney fails to participate in good faith and thereby causes additional expense.

**Failure of United States to Participate in Good Faith in Discovery.** Rule 37 authorizes the court to direct that parties or attorneys who fail to participate in good faith in the discovery process pay the expenses, including attorneys' fees, incurred by other parties as a result of that failure. Since attorneys' fees cannot ordinarily be awarded against the United States (28 U.S.C. § 2412), there is often no practical remedy for the misconduct of its officers and attorneys. However, in the case of a government attorney who fails to participate in good faith in discovery, nothing prevents a court in an appropriate case from giving written notification of that fact to the Attorney General of the United States and other appropriate heads of offices or agencies thereof.

**1987 Amendment**

The amendments are technical. No substantive change is intended.

**1993 Amendment**

**Subdivision (a).** This subdivision is revised to reflect the revision of Rule 26(a), requiring disclosure of matters without a discovery request.

Pursuant to new subdivision (a)(2)(A), a party dissatisfied with the disclosure made by an opposing party may under this rule move for an order to compel disclosure. In providing for such a motion, the revised rule parallels the provisions of the former rule dealing with failures to answer particular interrogatories. Such a motion may be needed when the information to be disclosed might be helpful to the party seeking the disclosure but not to the party required to make the disclosure. If the party required to make the disclosure would need the material to support its own contentions, the more effective enforcement of the disclosure requirement will be to exclude the evidence not disclosed, as provided in subdivision (c)(1) of this revised rule.

Language is included in the new paragraph and added to the subparagraph (B) that requires litigants to seek to resolve discovery disputes by informal means before filing a motion with the court. This requirement is based on successful experience with similar local rules of court promulgated pursuant to Rule 83.

The last sentence of paragraph (2) is moved into paragraph (4).

Under revised paragraph (3), evasive or incomplete disclosures and responses to interrogatories and production requests are treated as failures to disclose or respond. Interrogatories and requests for production should not be read or interpreted in an artificially restrictive or hypertechnical manner to avoid disclosure of information fairly covered by the discovery request, and to do so is subject to appropriate sanctions under subdivision (a).

Revised paragraph (4) is divided into three subparagraphs for ease of reference, and in each the phrase “after opportunity for hearing” is changed to “after affording an opportunity to be heard” to make clear that the court can consider such questions on written submissions as well as on oral hearings.

Subparagraph (A) is revised to cover the situation where information that should have been produced without a motion to compel is produced after the motion is filed but before it is brought on for hearing. The rule also is revised to provide

that a party should not be awarded its expenses for filing a motion that could have been avoided by conferring with opposing counsel.

Subparagraph (C) is revised to include the provision that formerly was contained in subdivision (a)(2) and to include the same requirement of an opportunity to be heard that is specified in subparagraphs (A) and (B).

**Subdivision (c).** The revision provides a self-executing sanction for failure to make a disclosure required by Rule 26(a), without need for a motion under subdivision (a)(2)(A).

Paragraph (1) prevents a party from using as evidence any witnesses or information that, without substantial justification, has not been disclosed as required by Rules 26(a) and 26(e)(1). This automatic sanction provides a strong inducement for disclosure of material that the disclosing party would expect to use as evidence, whether at a trial, at a hearing, or on a motion, such as one under Rule 56. As disclosure of evidence offered solely for impeachment purposes is not required under those rules, this preclusion sanction likewise does not apply to that evidence.

Limiting the automatic sanction to violations "without substantial justification," coupled with the exception for violations that are "harmless," is needed to avoid unduly harsh penalties in a variety of situations: *e.g.,* the inadvertent omission from a Rule 26(a)(1)(A) disclosure of the name of a potential witness known to all parties; the failure to list as a trial witness a person so listed by another party; or the lack of knowledge of a pro se litigant of the requirement to make disclosures. In the latter situation, however, exclusion would be proper if the requirement for disclosure had been called to the litigant's attention by either the court or another party.

Preclusion of evidence is not an effective incentive to compel disclosure of information that, being supportive of the position of the opposing party, might advantageously be concealed by the disclosing party. However, the rule provides the court with a wide range of other sanctions--such as declaring specified facts to be established, preventing contradictory evidence, or, like spoliation of evidence, allowing the jury to be informed of the fact of nondisclosure--that, though not self-executing, can be imposed when found to be warranted after a hearing. The failure to identify a witness or document in a disclosure statement would be admissible under the Federal Rules of Evidence under the same principles that allow a party's interrogatory answers to be offered against it.

**Subdivision (d).** This subdivision is revised to require that, where a party fails to file any response to interrogatories or a Rule 34 request, the discovering party should informally seek to obtain such responses before filing a motion for sanctions.

The last sentence of this subdivision is revised to clarify that it is the pendency of a motion for protective order that may be urged as an excuse for a violation of subdivision (d). If a party's motion has been denied, the party cannot argue that its subsequent failure to comply would be justified. In this connection, it should be noted that the filing of a motion under Rule 26(c) is not self-executing--the relief authorized under that rule depends on obtaining the court's order to that effect.

**Subdivision (g).** This subdivision is modified to conform to the revision of Rule 26(f).

**2000 Amendment**

**Subdivision (c)(1).** When this subdivision was added in 1993 to direct exclusion of materials not disclosed as required, the duty to supplement discovery responses pursuant to Rule 26(e)(2) was omitted. In the face of this omission, courts may rely on inherent power to sanction for failure to supplement as required by Rule 26(e)(2), *see 8 Federal Practice & Procedure* § 2050 at 607-09, but that is an uncertain and unregulated ground for imposing sanctions. There is no obvious occasion for a Rule 37(a) motion in connection with failure to supplement, and ordinarily only Rule 37(c)(1) exists as rule-based authority for sanctions if this supplementation obligation is violated.

The amendment explicitly adds failure to comply with Rule 26(e)(2) as a ground for sanctions under Rule 37(c)(1), including exclusion of withheld materials. The rule provides that this sanction power only applies when the failure to supplement was "without substantial justification." Even if the failure was not substantially justified, a party should be allowed to use the material that was not disclosed if the lack of earlier notice was harmless.

"Shall" is replaced by "is" under the program to conform amended rules to current style conventions when there is no ambiguity.

**GAP Report**

The Advisory Committee recommends that the published amendment proposal be modified to state that the exclusion sanction can apply to failure "to amend a prior response to discovery as required by Rule 26(e)(2)." In addition, one minor phrasing change is recommended for the Committee Note.

**2006 Amendment**

**Subdivision (f).** Subdivision (f) is new. It focuses on a distinctive feature of computer operations, the routine alteration and deletion of information that attends ordinary use. Many steps essential to computer operation may alter or destroy information, for reasons that have nothing to do with how that information might relate to litigation. As a result, the ordinary operation of computer systems creates a risk that a party may lose potentially discoverable information without culpable conduct on its part. Under Rule 37(f), absent exceptional circumstances, sanctions cannot be imposed for loss of electronically stored information resulting from the routine, good-faith operation of an electronic information system.

Rule 37(f) applies only to information lost due to the "routine operation of an electronic information system" -- the ways in which such systems are generally designed, programmed, and implemented to meet the party's technical and business needs. The "routine operation" of computer systems includes the alteration and overwriting of information, often without the operator's specific direction or awareness, a feature with no direct counterpart in hard-copy documents. Such features are essential to the operation of electronic information systems.

Rule 37(f) applies to information lost due to the routine operation of an information system only if the operation was in good faith. Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation. A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case. The good faith requirement of Rule 37(f) means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold." Among the factors that bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information.

Whether good faith would call for steps to prevent the loss of information on sources that the party believes are not reasonably accessible under Rule 26(b)(2) depends on the circumstances of each case. One factor is whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources.

The protection provided by Rule 37(f) applies only to sanctions "under these rules." It does not affect other sources of authority to impose sanctions or rules of professional responsibility.

This rule restricts the imposition of "sanctions." It does not prevent a court from making the kinds of adjustments frequently used in managing discovery if a party is unable to provide relevant responsive information. For example, a court could order the responding party to produce an additional witness for deposition, respond to additional interrogatories, or make similar attempts to provide substitutes or alternatives for some or all of the lost information.

**2007 Amendment**

The language of Rule 37 has been amended as part of the general restyling of the Civil Rules to make them more easily understood and to make style and terminology consistent throughout the rules. These changes are intended to be stylistic only.

**2013 Amendment**

Rule 37(b) is amended to conform to amendments made to Rule 45, particularly the addition of Rule 45(f) providing for transfer of a subpoena-related motion to the court where the action is pending. A second sentence is added to Rule 37(b)(1) to deal with contempt of orders entered after such a transfer. The Rule 45(f) transfer provision is explained in the Committee Note to Rule 45.

**Changes Made After Publication and Comment**

No changes were made after publication and comment.

**2015 Amendment**

**Subdivision (a).** Rule 37(a)(3)(B)(iv) is amended to reflect the common practice of producing copies of documents or electronically stored information rather than simply permitting inspection. This change brings item (iv) into line with paragraph (B), which provides a motion for an order compelling "production, or inspection."

**Subdivision (e).** Present Rule 37(e), adopted in 2006, provides: "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system." This limited rule has not adequately addressed the serious problems resulting from the continued exponential growth in the volume of such information. Federal circuits have established significantly different standards for imposing sanctions or curative measures on parties who fail to preserve electronically stored information. These developments have caused litigants to expend excessive effort and money on preservation in order to avoid the risk of severe sanctions if a court finds they did not do enough.

New Rule 37(e) replaces the 2006 rule. It authorizes and specifies measures a court may employ if information that should have been preserved is lost, and specifies the findings necessary to justify these measures. It therefore forecloses reliance on inherent authority or state law to determine when certain measures should be used. The rule does not affect the validity of an independent tort claim for spoliation if state law applies in a case and authorizes the claim.

The new rule applies only to electronically stored information, also the focus of the 2006 rule. It applies only when such information is lost. Because electronically stored information often exists in multiple locations, loss from one source may often be harmless when substitute information can be found elsewhere.

The new rule applies only if the lost information should have been preserved in the anticipation or conduct of litigation and the party failed to take reasonable steps to preserve it. Many court decisions hold that potential litigants have a duty to preserve relevant information when litigation is reasonably foreseeable. Rule 37(e) is based on this common-law

duty; it does not attempt to create a new duty to preserve. The rule does not apply when information is lost before a duty to preserve arises.

In applying the rule, a court may need to decide whether and when a duty to preserve arose. Courts should consider the extent to which a party was on notice that litigation was likely and that the information would be relevant. A variety of events may alert a party to the prospect of litigation. Often these events provide only limited information about that prospective litigation, however, so that the scope of information that should be preserved may remain uncertain. It is important not to be blinded to this reality by hindsight arising from familiarity with an action as it is actually filed.

Although the rule focuses on the common-law obligation to preserve in the anticipation or conduct of litigation, courts may sometimes consider whether there was an independent requirement that the lost information be preserved. Such requirements arise from many sources -- statutes, administrative regulations, an order in another case, or a party's own information-retention protocols. The court should be sensitive, however, to the fact that such independent preservation requirements may be addressed to a wide variety of concerns unrelated to the current litigation. The fact that a party had an independent obligation to preserve information does not necessarily mean that it had such a duty with respect to the litigation, and the fact that the party failed to observe some other preservation obligation does not itself prove that its efforts to preserve were not reasonable with respect to a particular case.

The duty to preserve may in some instances be triggered or clarified by a court order in the case. Preservation orders may become more common, in part because Rules 16(b)(3)(B)(iii) and 26(f)(3)(C) are amended to encourage discovery plans and orders that address preservation. Once litigation has commenced, if the parties cannot reach agreement about preservation issues, promptly seeking judicial guidance about the extent of reasonable preservation may be important.

The rule applies only if the information was lost because the party failed to take reasonable steps to preserve the information. Due to the ever-increasing volume of electronically stored information and the multitude of devices that generate such information, perfection in preserving all relevant electronically stored information is often impossible. As under the current rule, the routine, good-faith operation of an electronic information system would be a relevant factor for the court to consider in evaluating whether a party failed to take reasonable steps to preserve lost information, although the prospect of litigation may call for reasonable steps to preserve information by intervening in that routine operation. This rule recognizes that “reasonable steps” to preserve suffice; it does not call for perfection. The court should be sensitive to the party's sophistication with regard to litigation in evaluating preservation efforts; some litigants, particularly individual litigants, may be less familiar with preservation obligations than others who have considerable experience in litigation.

Because the rule calls only for reasonable steps to preserve, it is inapplicable when the loss of information occurs despite the party's reasonable steps to preserve. For example, the information may not be in the party's control. Or information the party has preserved may be destroyed by events outside the party's control -- the computer room may be flooded, a “cloud” service may fail, a malign software attack may disrupt a storage system, and so on. Courts may, however, need to assess the extent to which a party knew of and protected against such risks.

Another factor in evaluating the reasonableness of preservation efforts is proportionality. The court should be sensitive to party resources; aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff and resources to devote to those efforts. A party may act reasonably by choosing a less costly form of information preservation, if it is substantially as effective as more costly forms. It is important that counsel become familiar with their clients' information systems and digital data -- including social media -- to address these issues. A party urging that preservation requests are disproportionate may need to provide specifics about these matters in order to enable meaningful discussion of the appropriate preservation regime.

When a party fails to take reasonable steps to preserve electronically stored information that should have been preserved in the anticipation or conduct of litigation, and the information is lost as a result, Rule 37(e) directs that the initial focus should be on whether the lost information can be restored or replaced through additional discovery. Nothing in the rule limits the court's powers under Rules 16 and 26 to authorize additional discovery. Orders under Rule 26(b)(2)(B) regarding discovery from sources that would ordinarily be considered inaccessible or under Rule 26(c)(1)(B) on allocation of expenses may be pertinent to solving such problems. If the information is restored or replaced, no further measures should be taken. At the same time, it is important to emphasize that efforts to restore or replace lost information through discovery should be proportional to the apparent importance of the lost information to claims or defenses in the litigation. For example, substantial measures should not be employed to restore or replace information that is marginally relevant or duplicative.

**Subdivision (e)(1).** This subdivision applies only if information should have been preserved in the anticipation or conduct of litigation, a party failed to take reasonable steps to preserve the information, information was lost as a result, and the information could not be restored or replaced by additional discovery. In addition, a court may resort to (e)(1) measures only "upon finding prejudice to another party from loss of the information." An evaluation of prejudice from the loss of information necessarily includes an evaluation of the information's importance in the litigation.

The rule does not place a burden of proving or disproving prejudice on one party or the other. Determining the content of lost information may be a difficult task in some cases, and placing the burden of proving prejudice on the party that did not lose the information may be unfair. In other situations, however, the content of the lost information may be fairly evident, the information may appear to be unimportant, or the abundance of preserved information may appear sufficient to meet the needs of all parties. Requiring the party seeking curative measures to prove prejudice may be reasonable in such situations. The rule leaves judges with discretion to determine how best to assess prejudice in particular cases.

Once a finding of prejudice is made, the court is authorized to employ measures "no greater than necessary to cure the prejudice." The range of such measures is quite broad if they are necessary for this purpose. There is no all-purpose hierarchy of the severity of various measures; the severity of given measures must be calibrated in terms of their effect on the particular case. But authority to order measures no greater than necessary to cure prejudice does not require the court to adopt measures to cure every possible prejudicial effect. Much is entrusted to the court's discretion.

In an appropriate case, it may be that serious measures are necessary to cure prejudice found by the court, such as forbidding the party that failed to preserve information from putting on certain evidence, permitting the parties to present evidence and argument to the jury regarding the loss of information, or giving the jury instructions to assist in its evaluation of such evidence or argument, other than instructions to which subdivision (e)(2) applies. Care must be taken, however, to ensure that curative measures under subdivision (e)(1) do not have the effect of measures that are permitted under subdivision (e)(2) only on a finding of intent to deprive another party of the lost information's use in the litigation. An example of an inappropriate (e)(1) measure might be an order striking pleadings related to, or precluding a party from offering any evidence in support of, the central or only claim or defense in the case. On the other hand, it may be appropriate to exclude a specific item of evidence to offset prejudice caused by failure to preserve other evidence that might contradict the excluded item of evidence.

**Subdivision (e)(2).** This subdivision authorizes courts to use specified and very severe measures to address or deter failures to preserve electronically stored information, but only on finding that the party that lost the information acted with the intent to deprive another party of the information's use in the litigation. It is designed to provide a uniform standard in federal court for use of these serious measures when addressing failure to preserve electronically stored information. It rejects cases such as *Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99 (2d Cir. 2002), that authorize the giving of adverse-inference instructions on a finding of negligence or gross negligence.

Adverse-inference instructions were developed on the premise that a party's intentional loss or destruction of evidence to prevent its use in litigation gives rise to a reasonable inference that the evidence was unfavorable to the party responsible for loss or destruction of the evidence. Negligent or even grossly negligent behavior does not logically support that inference. Information lost through negligence may have been favorable to either party, including the party that lost it, and inferring that it was unfavorable to that party may tip the balance at trial in ways the lost information never would have. The better rule for the negligent or grossly negligent loss of electronically stored information is to preserve a broad range of measures to cure prejudice caused by its loss, but to limit the most severe measures to instances of intentional loss or destruction.

Similar reasons apply to limiting the court's authority to presume or infer that the lost information was unfavorable to the party who lost it when ruling on a pretrial motion or presiding at a bench trial. Subdivision (e)(2) limits the ability of courts to draw adverse inferences based on the loss of information in these circumstances, permitting them only when a court finds that the information was lost with the intent to prevent its use in litigation.

Subdivision (e)(2) applies to jury instructions that permit or require the jury to presume or infer that lost information was unfavorable to the party that lost it. Thus, it covers any instruction that directs or permits the jury to infer from the loss of information that it was in fact unfavorable to the party that lost it. The subdivision does not apply to jury instructions that do not involve such an inference. For example, subdivision (e)(2) would not prohibit a court from allowing the parties to present evidence to the jury concerning the loss and likely relevance of information and instructing the jury that it may consider that evidence, along with all the other evidence in the case, in making its decision. These measures, which would not involve instructing a jury it may draw an adverse inference from loss of information, would be available under subdivision (e)(1) if no greater than necessary to cure prejudice. In addition, subdivision (e)(2) does not limit the discretion of courts to give traditional missing evidence instructions based on a party's failure to present evidence it has in its possession at the time of trial.

Subdivision (e)(2) requires a finding that the party acted with the intent to deprive another party of the information's use in the litigation. This finding may be made by the court when ruling on a pretrial motion, when presiding at a bench trial, or when deciding whether to give an adverse inference instruction at trial. If a court were to conclude that the intent finding should be made by a jury, the court's instruction should make clear that the jury may infer from the loss of the information that it was unfavorable to the party that lost it only if the jury first finds that the party acted with the intent to deprive another party of the information's use in the litigation. If the jury does not make this finding, it may not infer from the loss that the information was unfavorable to the party that lost it.

Subdivision (e)(2) does not include a requirement that the court find prejudice to the party deprived of the information. This is because the finding of intent required by the subdivision can support not only an inference that the lost information was unfavorable to the party that intentionally destroyed it, but also an inference that the opposing party was prejudiced by the loss of information that would have favored its position. Subdivision (e)(2) does not require any further finding of prejudice.

Courts should exercise caution, however, in using the measures specified in (e)(2). Finding an intent to deprive another party of the lost information's use in the litigation does not require a court to adopt any of the measures listed in subdivision (e)(2). The remedy should fit the wrong, and the severe measures authorized by this subdivision should not be used when the information lost was relatively unimportant or lesser measures such as those specified in subdivision (e)(1) would be sufficient to redress the loss.

Notes of Decisions (2938)

Fed. Rules Civ. Proc. Rule 37, 28 U.S.C.A., FRCP Rule 37

Including Amendments Received Through 9-1-17

**End of Document**

**NEW YORK STATE**
**DEPARTMENT OF FINANCIAL SERVICES**
**23 NYCRR 500**

# CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

I, Maria T. Vullo, Superintendent of Financial Services, pursuant to the authority granted by sections 102, 201, 202, 301, 302 and 408 of the Financial Services Law, do hereby promulgate Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect March 1, 2017, to read as follows:

**(ALL MATTER IS NEW)**

## Section 500.00 Introduction.

The New York State Department of Financial Services ("DFS") has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cybersecurity threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

## Section 500.01 Definitions.

For purposes of this Part only, the following definitions shall apply:

(a) *Affiliate* means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.

(b) *Authorized User* means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

(c) *Covered Entity* means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.

(d) *Cybersecurity Event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

(e) *Information System* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

(f) *Multi-Factor Authentication* means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password; or

(2) Possession factors, such as a token or text message on a mobile phone; or

(3) Inherence factors, such as a biometric characteristic.

(g) *Nonpublic Information* shall mean all electronic information that is not Publicly Available Information and is:

(1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;

(2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records;

(3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

(h) *Penetration Testing* means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems.

(i) *Person* means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

(j) *Publicly Available Information* means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

(1) For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(k) *Risk Assessment* means the risk assessment that each Covered Entity is required to conduct under section 500.09 of this Part.

(l) *Risk-Based Authentication* means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

(m) *Senior Officer(s)* means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part.

(n) *Third Party Service Provider(s)* means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

**Section 500.02 Cybersecurity Program.**

(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.

(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

(3) detect Cybersecurity Events;

(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;

(5) recover from Cybersecurity Events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

(c) A Covered Entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the Covered Entity.

(d) All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

**Section 500.03 Cybersecurity Policy.**

Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations:

(a) information security;

(b) data governance and classification;

(c) asset inventory and device management;

(d) access controls and identity management;

(e) business continuity and disaster recovery planning and resources;

(f) systems operations and availability concerns;

(g) systems and network security;

(h) systems and network monitoring;

(i) systems and application development and quality assurance;

(j) physical security and environmental controls;

(k) customer data privacy;

(l) vendor and Third Party Service Provider management;

(m) risk assessment; and

(n) incident response.

**Section 500.04 Chief Information Security Officer.**

(a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, "Chief Information Security Officer" or "CISO"). The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using a Third Party Service Provider or an Affiliate, the Covered Entity shall:

(1) retain responsibility for compliance with this Part;

(2) designate a senior member of the Covered Entity's personnel responsible for direction and oversight of the Third Party Service Provider; and

(3) require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity in accordance with the requirements of this Part.

(b) Report. The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable:

(1) the confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems;

(2) the Covered Entity's cybersecurity policies and procedures;

(3) material cybersecurity risks to the Covered Entity;

(4) overall effectiveness of the Covered Entity's cybersecurity program; and

(5) material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.

**Section 500.05 Penetration Testing and Vulnerability Assessments.**

The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

(a) annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

(b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

**Section 500.06 Audit Trail.**

(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:

(1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and

(2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.

(b) Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.

**Section 500.07 Access Privileges.**

As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

**Section 500.08 Application Security.**

(a) Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.

(b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.

**Section 500.09 Risk Assessment.**

(a) Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.

(b) The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;

(2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

**Section 500.10 Cybersecurity Personnel and Intelligence.**

(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall:

(1) utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.02(b)(1)-(6) of this Part;

(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

(b) A Covered Entity may choose to utilize an Affiliate or qualified Third Party Service Provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.

**Section 500.11 Third Party Service Provider Security Policy.**

(a) Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible

to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:

(1) the identification and risk assessment of Third Party Service Providers;

(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and

(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:

(1) the Third Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information;

(2) the Third Party Service Provider's policies and procedures for use of encryption as required by section 500.15 of this Part to protect Nonpublic Information in transit and at rest;

(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third Party Service Provider; and

(4) representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.

(c) Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.

**Section 500.12 Multi-Factor Authentication**.

(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.

(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

**Section 500.13 Limitations on Data Retention.**

As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information identified in section 500.01(g)(2)-(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

**Section 500.14 Training and Monitoring.**

As part of its cybersecurity program, each Covered Entity shall:

(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and

(b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

**Section 500.15 Encryption of Nonpublic Information.**

(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.

(1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(b) To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

**Section 500.16 Incident Response Plan.**

(a) As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.

(b) Such incident response plan shall address the following areas:

(1) the internal processes for responding to a Cybersecurity Event;

(2) the goals of the incident response plan;

(3) the definition of clear roles, responsibilities and levels of decision-making authority;

(4) external and internal communications and information sharing;

(5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;

(6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and

(7) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

**Section 500.17 Notices to Superintendent.**

(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

(1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or

(2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

(b) Annually each Covered Entity shall submit to the superintendent a written statement covering the prior calendar year. This statement shall be submitted by February 15 in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent.

**Section 500.18 Confidentiality.**

Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.

**Section 500.19 Exemptions.**

(a) Limited Exemption. Each Covered Entity with:

(1) fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity, or

(2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates, or

(3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates,

shall be exempt from the requirements of sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(b) An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity.

(c) A Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(d) A Covered Entity under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates) shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(e) A Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption in the form set forth as Appendix B within 30 days of the determination that the Covered Entity is exempt.

(f) The following Persons are exempt from the requirements of this Part, provided such Persons do not otherwise qualify as a Covered Entity for purposes of this Part: Persons subject to Insurance Law section 1110; Persons subject to Insurance Law section 5904; and any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125.

(g) In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, such Covered Entity shall have 180 days from such fiscal year end to comply with all applicable requirements of this Part.

**Section 500.20 Enforcement.**

This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.

**Section 500.21 Effective Date.**

This Part will be effective March 1, 2017. Covered Entities will be required to annually prepare and submit to the superintendent a Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations under section 500.17(b) of this Part commencing February 15, 2018.

**Section 500.22 Transitional Periods.**

(a) Transitional Period. Covered Entities shall have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified.

(b) The following provisions shall include additional transitional periods. Covered Entities shall have:

(1) One year from the effective date of this Part to comply with the requirements of sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(b) of this Part.

(2) Eighteen months from the effective date of this Part to comply with the requirements of sections 500.06, 500.08, 500.13, 500.14 (a) and 500.15 of this Part.

(3) Two years from the effective date of this Part to comply with the requirements of section 500.11 of this Part.

**Section 500.23 Severability.**

If any provision of this Part or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other Persons or circumstances.

APPENDIX A (Part 500)

(**Covered Entity Name)**

**February 15, 20_____**

**Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations**

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of_____(date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended__(year for which Board Resolution or Compliance Finding is provided) complies with Part ___.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name)_____ Date: _____

[DFS Portal Filing Instructions]

APPENDIX B (Part 500)

(**Covered Entity Name)**

**(Date)_____**

**Notice of Exemption**

In accordance with 23 NYCRR § 500.19(e), (Covered Entity Name) hereby provides notice that (Covered Entity Name) qualifies for the following Exemption(s) under 23 NYCRR § 500.19 (check all that apply):

- ☐ Section 500.19(a)(1)
- ☐ Section 500.19(a)(2)
- ☐ Section 500.19(a)(3)
- ☐ Section 500.19(b)
- ☐ Section 500.19(c)
- ☐ Section 500.19(d)

If you have any question or concerns regarding this notice, please contact:

(Insert name, title, and full contact information)

(Name)_____ Date: _____

(Title)

(Covered Entity Name)

[DFS Portal Filing Instructions]

NEW YORK STATE
DEPARTMENT *of*
FINANCIAL SERVICES

Andrew M. Cuomo
Governor

Maria T. Vullo
Superintendent

# CERTIFICATION

I, Maria T. Vullo, Superintendent of Financial Services, do hereby certify that the attached new Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect upon publication in the State Register, has been duly adopted by me on the date set forth below pursuant to authority vested in the Department of Financial Services by Sections 102, 201, 202, 301, 302 and 408 of the Financial Services Law.

The notice of proposed rule making for this amendment was published in the State Register on September 28, 2016 under ID No. DFS-39-16-00008-P. A notice of revised proposed rule making for this amendment was published in the State Register on December 28, 2016 under ID No. DFS-39-16-00008-RP. No other publication of prior notice was required by statute.

Date: February 13, 2017

Mario T. Vullo
Superintendent of Financial Services

# PROTECTING PERSONAL INFORMATION

## A Guide for Business

Federal Trade Commission | business.ftc.gov

Most companies keep sensitive personal information in their files—names, Social Security numbers, credit card, or other account data—that identifies customers or employees.

This information often is necessary to fill orders, meet payroll, or perform other necessary business functions. However, if sensitive data falls into the wrong hands, it can lead to fraud, identity theft, or similar harms. Given the cost of a security breach—losing your customers' trust and perhaps even defending yourself against a lawsuit—safeguarding personal information is just plain good business.

Some businesses may have the expertise in-house to implement an appropriate plan. Others may find it helpful to hire a contractor. Regardless of the size—or nature—of your business, the principles in this brochure will go a long way toward helping you keep data secure.

A sound data security plan is built on 5 key principles:

## 1. TAKE STOCK.

Know what personal information you have in your files and on your computers.

## 2. SCALE DOWN.

Keep only what you need for your business.

## 3. LOCK IT.

Protect the information that you keep.

## 4. PITCH IT.

Properly dispose of what you no longer need.

## 5. PLAN AHEAD.

Create a plan to respond to security incidents.

Use the checklists on the following pages to see how your company's practices measure up—and where changes are necessary.

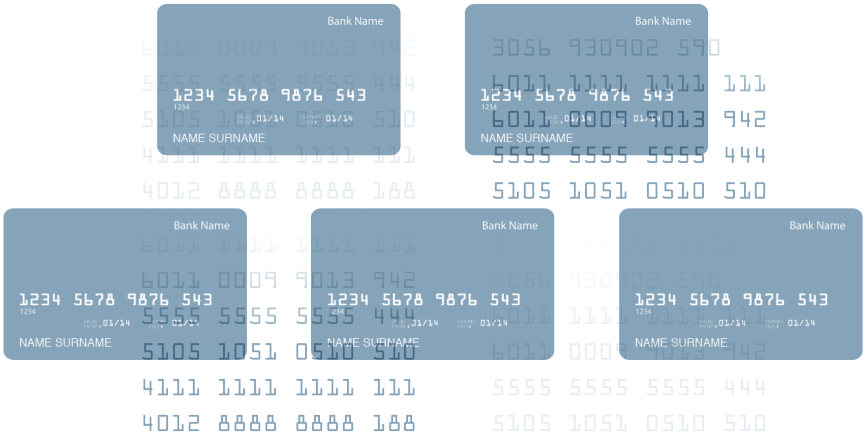
# 1. TAKE STOCK.

## Know what personal information you have in your files and on your computers.

Effective data security starts with assessing what information you have and identifying who has access to it. Understanding how personal information moves into, through, and out of your business and who has—or could have—access to it is essential to assessing security vulnerabilities. You can determine the best ways to secure the information only after you've traced how it flows.

- Inventory all computers, laptops, mobile devices, flash drives, disks, home computers, digital copiers, and other equipment to find out where your company stores sensitive data. Also, inventory the information you have by type and location. Your file cabinets and computer systems are a start, but remember: your business receives personal information in a number of ways—through websites, from contractors, from call centers, and the like. What about information saved on laptops, employees' home computers, flash drives, digital copiers, and mobile devices? No inventory is complete until you check everywhere sensitive data might be stored.

- Track personal information through your business by talking with your sales department, information technology staff, human resources office, accounting personnel, and outside service providers. Get a complete picture of:
  - **Who sends sensitive personal information to your business.** Do you get it from customers? Credit card companies? Banks or other financial institutions? Credit bureaus? Job applicants? Other businesses?
  - **How your business receives personal information.** Does it come to your business through a website? By email? Through the mail? Is it transmitted through cash registers in stores?




  - **What kind of information you collect at each entry point.** Do you get credit card information online? Does your accounting department keep information about customers' checking accounts?

- **Where you keep the information you collect at each entry point**. Is it in a central computer database? On individual laptops? On a cloud computing service? On employees' smartphones, tablets, or other mobile devices? On disks or tapes? In file cabinets? In branch offices? Do employees have files at home?

## SECURITY CHECK

**Question:**
Are there laws that require my company to keep sensitive data secure?

**Answer:**
Yes. While you're taking stock of the data in your files, take stock of the law, too. Statutes like the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Federal Trade Commission Act may require you to provide reasonable security for sensitive information.

To find out more, visit **business.ftc.gov/privacy-and-security**

- Who has—or could have—access to the information? Which of your employees has permission to access the information? Do they need access? Could anyone else get hold of it? What about vendors who supply and update software you use to process credit card transactions? Contractors operating your call center?
- Different types of information present varying risks. Pay particular attention to how you keep personally identifying information: Social Security numbers, credit card or financial information, and other sensitive data. That's what thieves use most often to commit fraud or identity theft.

## 2. SCALE DOWN.

### Keep only what you need for your business.

If you don't have a legitimate business need for sensitive personally identifying information, don't keep it. In fact, don't even collect it. If you have a legitimate business need for the information, keep it only as long as it's necessary.

- Use Social Security numbers only for required and lawful purposes—like reporting employee taxes. Don't use Social Security numbers unnecessarily—for example, as an employee or customer identification number, or because you've always done it.

### SECURITY CHECK

**Question:**
We like to have accurate information about our customers, so we usually create a permanent file about all aspects of their transactions, including the information we collect from the magnetic stripe on their credit cards. Could this put their information at risk?

**Answer:**
Yes. Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not in your system, it can't be stolen by hackers.

- If your company develops a mobile app, make sure the app accesses only the data and functionality that it needs. And don't collect and retain personal information unless it's integral to your product or service. Remember, if you collect and retain data, you must protect it.
- Don't keep customer credit card information unless you have a business need for it. For example, don't retain the account number and expiration date unless you have an essential business need to do so. Keeping this information—or keeping it longer than necessary—raises the risk that the information could be used to commit fraud or identity theft.
- Scale down access to data. Follow the "principle of least privilege." That means each employee should have access only to those resources needed to do their particular job.

If you must keep information for business reasons, or to comply with the law, develop a written records retention policy to identify what information must be kept, how to secure it, how long to keep it, and how to dispose of it securely when you no longer need it.

# 3. LOCK IT.

## Protect the information that you keep.

What's the best way to protect the sensitive personally identifying information you need to keep? It depends on the kind of information and how it's stored. The most effective data security plans deal with four key elements: physical security, electronic security, employee training, and the security practices of contractors and service providers.

### *Physical Security*

Many data compromises happen the old-fashioned way—through lost or stolen paper documents. Often, the best defense is a locked door or an alert employee.

- Store paper documents or files, as well as thumb drives and backups containing personally identifiable information, in a locked room or in a locked file cabinet. Limit access to employees with a legitimate business need. Control who has a key, and the number of keys.
- Require that files containing personally identifiable information be kept in locked file cabinets except when an employee is working on the file. Remind employees not to leave sensitive papers out on their desks when they are away from their workstations.
- Require employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.

- Implement appropriate access controls for your building. Tell employees what to do and whom to call if they see an unfamiliar person on the premises.
- If you maintain offsite storage facilities, limit employee access to those with a legitimate business need. Know if and when someone accesses the storage site.
- If you ship sensitive information using outside carriers or contractors, encrypt the information and keep an inventory of the information being shipped. Also use an overnight shipping service that will allow you to track the delivery of your information.
- If you have devices that collect sensitive information, like PIN pads, secure them so that identity thieves can't tamper with them. Also, inventory those items to ensure that they have not been switched.

## *Electronic Security*

Computer security isn't just the realm of your IT staff. Make it your business to understand the vulnerabilities of your computer system, and follow the advice of experts in the field.

## *General Network Security*

- Identify the computers or servers where sensitive personal information is stored.
- Identify all connections to the computers where you store sensitive information. These may include the internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, digital copiers, and wireless devices like smartphones, tablets, or inventory scanners.

- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.
- Don't store sensitive consumer data on any computer with an internet connection unless it's essential for conducting your business.

- Encrypt sensitive information that you send to third parties over public networks (like the internet), and encrypt sensitive information that is stored on your computer network, laptops, or portable storage devices used by your employees. Consider also encrypting email transmissions within your business.
- Regularly run up-to-date anti-malware programs on individual computers and on servers on your network.
- Check expert websites (such as www.us-cert.gov) and your software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches to correct problems.

## 3 Lock It

- Restrict employees' ability to download unauthorized software. Software downloaded to devices that connect to your network (computers, smartphones, and tablets) could be used to distribute malware.
- Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
- When you receive or transmit credit card information or other sensitive financial data, use Transport Layer Security (TLS) encryption or another secure connection that protects the information in transit.

- Pay particular attention to the security of your web applications—the software used to give information to visitors to your website and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks. In one variation called an "injection attack," a hacker inserts malicious commands into what looks like a legitimate request for information. Once in your system, hackers transfer sensitive information from your network to their computers. Relatively simple defenses against these attacks are available from a variety of sources.

## SECURITY CHECK

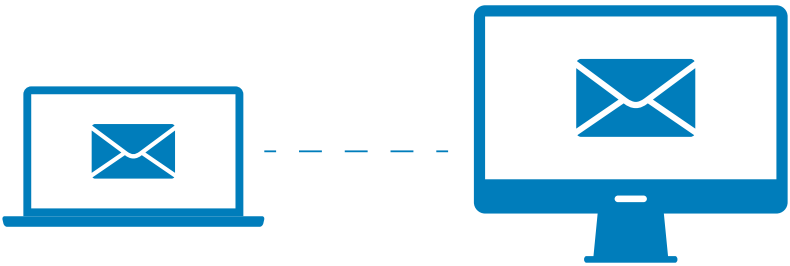
**Question:**
We encrypt the financial data customers submit on our website. But once we receive it, we decrypt it and email it over the internet to our branch offices in regular text. Is there a safer practice?

**Answer:**
Yes. Regular email is not a secure method for sending sensitive data. The better practice is to encrypt any transmission that contains information that could be used by fraudsters or identity thieves.

## *Authentication*

- Control access to sensitive information by requiring that employees use "strong" passwords. Tech security experts say the longer the password, the better. Because simple passwords—like common dictionary words—can be guessed easily, insist that employees choose passwords with a mix of letters, numbers, and characters. Require an employee's user name and password to be different. Require password changes when appropriate—for example, following a breach.
  - Consider using multi-factor authentication, such as requiring the use of a password and a code sent by different methods.
- Explain to employees why it's against company policy to share their passwords or post them near their workstations.
- Use password-activated screen savers to lock employee computers after a period of inactivity.
- Lock out users who don't enter the correct password within a designated number of log-on attempts.
- Warn employees about possible calls from identity thieves attempting to deceive them into giving out their passwords by impersonating members of your IT staff. Let employees know that calls like this are always fraudulent, and that no one should be asking them to reveal their passwords.

- When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
- Caution employees against transmitting sensitive personally identifying data—Social Security numbers, passwords, account information—via email. Unencrypted email is not a secure way to transmit information.

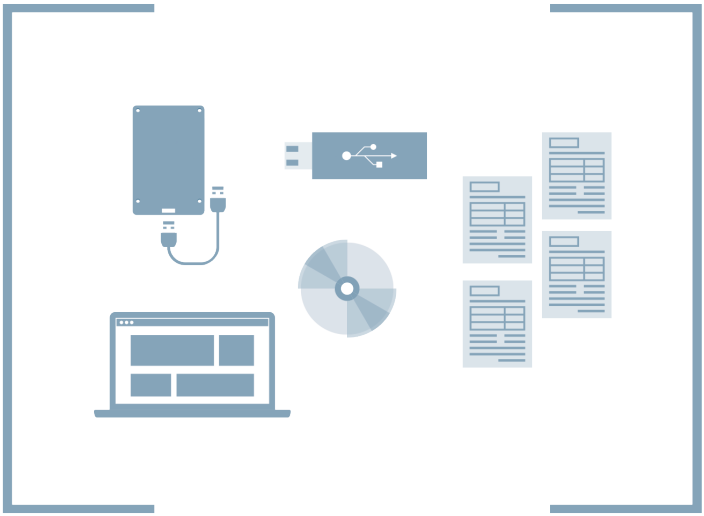


## *Laptop Security*

- Restrict the use of laptops to those employees who need them to perform their jobs.
- Assess whether sensitive information really needs to be stored on a laptop. If not, delete it with a "wiping" program that overwrites data on the laptop. Deleting files using standard keyboard commands isn't sufficient because data may remain on the laptop's hard drive. Wiping programs are available at most office supply stores.
- Require employees to store laptops in a secure place. Even when laptops are in use, consider using cords and locks to secure laptops to employees' desks.

- Consider allowing laptop users to only access sensitive information, but not to store the information on their laptops. Under this approach, the information is stored on a secure central computer and the laptops function as terminals that display information from the central computer, but do not store it. The information could be further protected by requiring the use of a token, "smart card," thumb print, or other biometric—as well as a password—to access the central computer.

- If a laptop contains sensitive data, encrypt it and configure it so users can't download any software or change the security settings without approval from your IT specialists. Consider adding an "auto-destroy" function so that data on a computer that is reported stolen will be destroyed when the thief uses the computer to try to get on the internet.
- Train employees to be mindful of security when they're on the road. They should never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage unless directed to by airport security. If someone must leave a laptop in a car, it should be locked in a trunk. Everyone who goes through airport security should keep an eye on their laptop as it goes on the belt.



## SECURITY CHECK

**Question:**
Our account staff needs access to our database of customer financial information. To make it easier to remember, we just use our company name as the password. Could that create a security problem?

**Answer:**
Yes. Hackers will first try words like “password,” your company name, the software’s default password, and other easy-to-guess choices. They’ll also use programs that run through common English words and dates. To make it harder for them to crack your system, select strong passwords—the longer, the better—that use a combination of letters, symbols, and numbers. Don’t store passwords in clear text. Use a password management system that adds salt—random data—to hashed passwords and consider using slow hash functions.

### *Firewalls*

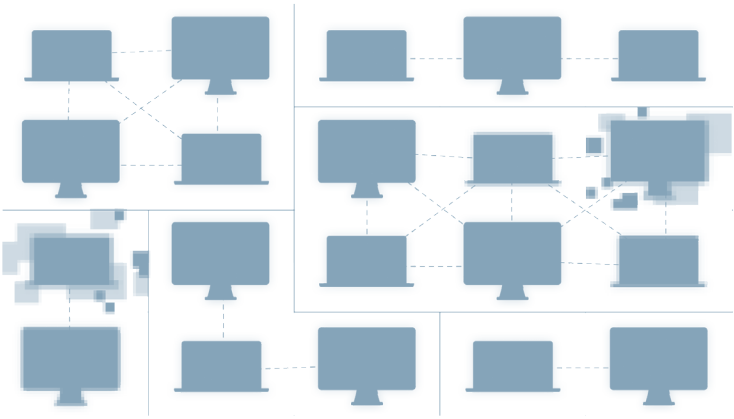
- Use a firewall to protect your computer from hacker attacks while it is connected to a network, especially the internet. A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files.

- Determine whether you should install a “border” firewall where your network connects to the internet. A border firewall separates your network from the internet and may prevent an attacker from gaining access to a computer on the network where you store sensitive information. Set “access controls”—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, review them periodically.
- If some computers on your network store sensitive information while others do not, consider using additional firewalls to protect the computers with sensitive information.

## *Wireless and Remote Access*

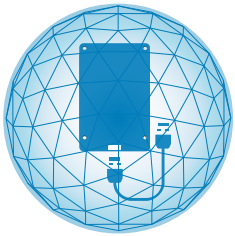
- Determine if you use wireless devices like smartphones, tablets, or inventory scanners or cell phones to connect to your computer network or to transmit sensitive information.

- If you do, consider limiting who can use a wireless connection to access your computer network. You can make it harder for an intruder to access the network by limiting the wireless devices that can connect to your network.



- Encrypt the information you send over your wireless network, so that nearby attackers can't eavesdrop on these communications. Look for a wireless router that has Wi-Fi Protected Access 2 (WPA2) capability and devices that support WPA2.
- Use encryption if you allow remote access to your computer network by employees or by service providers, such as companies that troubleshoot and update software you use to process credit card purchases. Consider implementing multi-factor authentication for access to your network.

## *Digital Copiers*



Your information security plan should cover the digital copiers your company uses. The hard drive in a digital copier stores data about the documents it copies, prints, scans, faxes, or emails. If you don't take steps to protect that data, it can be stolen from the hard drive, either by remote access or by extraction once the drive has been removed.

Here are some tips about safeguards for sensitive data stored on the hard drives of digital copiers:

- Get your IT staff involved when you're thinking about getting a copier. Employees responsible for securing your computers also should be responsible for securing data on digital copiers.
- When you're buying or leasing a copier, consider data security features offered, either as standard equipment or as optional add-on kits. Typically, these features involve encryption and overwriting. Encryption scrambles the data on the hard drive so it can be read only by particular software. Overwriting—also known as file wiping or shredding—replaces the existing data with random characters, making it harder for someone to reconstruct a file.

- Once you choose a copier, take advantage of all its security features. You may be able to set the number of times data is overwritten—generally, the more times the data is overwritten, the safer it is from being retrieved. In addition, make it an office practice to securely overwrite the entire hard drive at least once a month.
- When you return or dispose of a copier, find out whether you can have the hard drive removed and destroyed, or overwrite the data on the hard drive. Have a skilled technician remove the hard drive to avoid the risk of breaking the machine.

To find out more, read *Copier Data Security: A Guide for Businesses* at ftc.gov/privacy-and-security (click on Data Security).

## *Detecting Breaches*

- To detect network breaches when they occur, consider using an intrusion detection system. To be effective, it must be updated frequently to address new types of hacking.
- Maintain central log files of security-related information to monitor activity on your network so that you can spot and respond to attacks. If there is an attack on your network, the log will provide information that can identify the computers that have been compromised.

- Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.
- Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from your system to an unknown user. If large amounts of information are being transmitted from your network, investigate to make sure the transmission is authorized.
- Have in place and implement a breach response plan. See page 30 for more information.

## SECURITY CHECK

**Question:**
I'm not really a "tech" type. Are there steps our computer people can take to protect our system from common hack attacks?

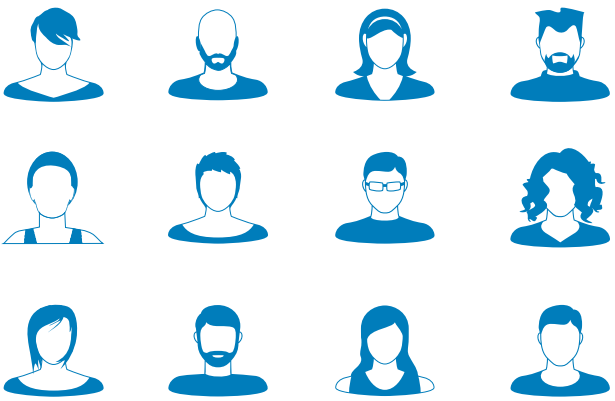
**Answer:**
Yes. There are simple fixes to protect your computers from some of the most common vulnerabilities. For example, a threat called an "SQL injection attack" can give fraudsters access to sensitive data on your system.

Protect your systems by keeping software updated and conducting periodic security reviews for your network. Bookmark the websites of groups like the Open Web Application Security Project, **www.owasp.org**, or SANS (SysAdmin, Audit, Network, Security) Institute's *The Top Cyber Security Risks*, **www.sans.org/top20**, for up-to-date information on the latest threats—and fixes. And check with your software vendors for patches that address new vulnerabilities. For more tips on keeping sensitive data secure, read *Start with Security: A Guide for Business* at **ftc.gov/startwithsecurity**.

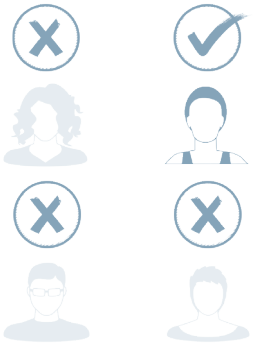
## *Employee Training*

Your data security plan may look great on paper, but it's only as strong as the employees who implement it. Take time to explain the rules to your staff, and train them to spot security vulnerabilities. Periodic training emphasizes the importance you place on meaningful data security practices. A well-trained workforce is the best defense against identity theft and data breaches.

- Check references or do background checks before hiring employees who will have access to sensitive data.
- Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling sensitive data. Make sure they understand that abiding by your company's data security plan is an essential part of their duties.
- Regularly remind employees of your company's policy—and any legal requirement—to keep customer information secure and confidential.



- Know which employees have access to consumers' sensitive personally identifying information. Pay particular attention to data like Social Security numbers and account numbers. Limit access to personal information to employees with a "need to know."
- Have a procedure in place for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information. Terminate their passwords and collect keys and identification cards as part of the check-out routine.



- Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. Make sure training includes employees at satellite offices, temporary help, and seasonal workers. If employees don't attend, consider blocking their access to the network.
- Train employees to recognize security threats. Tell them how to report suspicious activity and publicly reward employees who alert you to vulnerabilities. Visit ftc.gov/startwithsecurity to show them videos on vulnerabilities that could affect your company, along with practical guidance on how to reduce data security risks.

- Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate. Make sure your policies cover employees who telecommute or access sensitive data from home or an offsite location.
- Teach employees about the dangers of spear phishing—emails containing information that makes the emails look legitimate. These emails may appear to come from someone within your company, generally someone in a position of authority. Make it office policy to independently verify any emails requesting sensitive information. When verifying, do not reply to the email and do not use links, phone numbers, or websites contained in the email.
- Warn employees about phone phishing. Train them to be suspicious of unknown callers claiming to need account numbers to process an order or asking for customer or employee contact information. Make it office policy to double-check by contacting the company using a phone number you know is genuine.
- Require employees to notify you immediately if there is a potential security breach, such as a lost or stolen laptop.
- Impose disciplinary measures for security policy violations.
- For computer security tips, tutorials, and quizzes for everyone on your staff, visit www.ftc.gov/OnGuardOnline.

## *Security Practices of Contractors and Service Providers*

Your company's security practices depend on the people who implement them, including contractors and service providers.

- Before you outsource any of your business functions—payroll, web hosting, customer call center operations, data processing, or the like—investigate the company's data security practices and compare their standards to yours. If possible, visit their facilities.
- Put your security expectations in writing in contracts with service providers. Then, don't just take their word for it—verify compliance.
- Insist that your service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of your data.

## 4. PITCH IT.

### Properly dispose of what you no longer need.

What looks like a sack of trash to you can be a gold mine for an identity thief. Leaving credit card receipts or papers or CDs with personally identifying information in a dumpster facilitates fraud and exposes consumers to the risk of identity theft. By properly disposing of sensitive information, you ensure that it cannot be read or reconstructed.

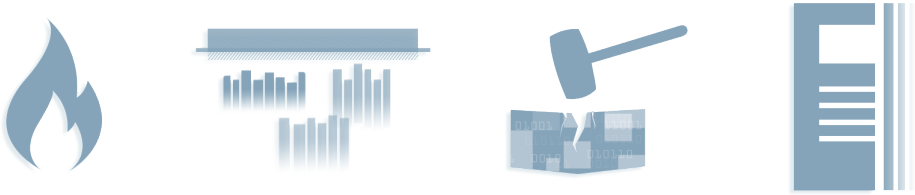
- Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to—or use of—personally identifying information. Reasonable measures for your operation are based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.

**SECURITY CHECK**

**Question:**
My company collects credit applications from customers. The form requires them to give us lots of financial information. Once we're finished with the applications, we're careful to throw them away. Is that sufficient?

**Answer:**
No. Have a policy in place to ensure that sensitive paperwork is unreadable before you throw it away. Burn it, shred it, or pulverize it to make sure identity thieves can't steal it from your trash.

## 4 Pitch It



- Effectively dispose of paper records by shredding, burning, or pulverizing them before discarding. Make shredders available throughout the workplace, including next to the photocopier.
- When disposing of old computers and portable storage devices, use software for securely erasing data, usually called wipe utility programs. They're inexpensive and can provide better results by overwriting the entire hard drive so that the files are no longer recoverable. Deleting files using the keyboard or mouse commands usually isn't sufficient because the files may continue to exist on the computer's hard drive and could be retrieved easily.
- Make sure employees who work from home follow the same procedures for disposing of sensitive documents and old computers and portable storage devices.
- If you use consumer credit reports for a business purpose, you may be subject to the FTC's Disposal Rule. For more information, see *Disposing of Consumer Report Information? Rule Tells How* at ftc.gov/privacy-and-security (click on Credit Reporting).

# 5. PLAN AHEAD.

## Create a plan for responding to security incidents.

Taking steps to protect data in your possession can go a long way toward preventing a security breach. Nevertheless, breaches can happen. Here's how you can reduce the impact on your business, your employees, and your customers:

- Have a plan in place to respond to security incidents. Designate a senior member of your staff to coordinate and implement the response plan.
- If a computer is compromised, disconnect it immediately from your network.
- Investigate security incidents immediately and take steps to close off existing vulnerabilities or threats to personal information.
- Consider whom to notify in the event of an incident, both inside and outside your organization. You may need to notify consumers, law enforcement, customers, credit bureaus, and other businesses that may be affected by the breach. In addition, many states and the federal bank regulatory agencies have laws or guidelines addressing data breaches. Consult your attorney.

## SECURITY CHECK

**Question:**
I own a small business. Aren't these precautions going to cost me a mint to implement?

**Answer:**
No. There's no one-size-fits-all approach to data security, and what's right for you depends on the nature of your business and the kind of information you collect from your customers. Some of the most effective security measures—using strong passwords, locking up sensitive paperwork, training your staff, etc.—will cost you next to nothing and you'll find free or low-cost security tools at non-profit websites dedicated to data security. Furthermore, it's cheaper in the long run to invest in better data security than to lose the goodwill of your customers, defend yourself in legal actions, and face other possible consequences of a data breach.

## Additional Resources

These websites and publications have more information on securing sensitive data:

**Start with Security**
www.ftc.gov/startwithsecurity

**National Institute of Standards and Technology (NIST) Computer Security Resource Center**
www.csrc.nist.gov

**SANS (SysAdmin, Audit, Network, Security) Institute Critical Security Controls**
www.sans.org/top20

**United States Computer Emergency Readiness Team (US-CERT)**
www.us-cert.gov

**OnGuard Online**
www.ftc.gov/OnGuardOnline

**Small Business Administration**
www.sba.gov/cybersecurity

**Better Business Bureau**
www.bbb.org/cybersecurity

## About the FTC

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace and to provide information to businesses to help them comply with the law. For free compliance resources visit the Business Center at business.ftc.gov.

## Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

Federal Trade Commission
**business.ftc.gov**
October 2016

I

*(Legislative acts)*

# REGULATIONS

## REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

## of 27 April 2016

## on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

**(Text with EEA relevance)**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

Having regard to the opinion of the Committee of the Regions ([2]),

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council ([4]) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

([1]) OJ C 229, 31.7.2012, p. 90.
([2]) OJ C 391, 18.12.2012, p. 127.
([3]) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
([4]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

(5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

(8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.

(9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

(11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

(12) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC ([1]).

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council ([2]) applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or

([1]) Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).

([2]) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

(19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council ([1]). Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

(20) While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council ([2]), in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

(22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

([1]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (see page 89 of this Official Journal).

([2]) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council ([1]) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be

([1]) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or

Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC ([1]) a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

(45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data

([1]) Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their

further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes

by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council ([1]), namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(57) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

([1]) Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given

his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

(67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(69) Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

(72) Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.

(73) Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(80) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the

nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes

aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

(90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data

protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out

and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

(99) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

(100) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of

protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

(106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council ([1]) as established under this Regulation, to the European Parliament and to the Council.

(107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the

([1]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

(110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(111) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.

(112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

(113) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

(115) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.

(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.

(119) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.

(120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(121) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.

(122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the

processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

(123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

(124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.

(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

(126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision *vis-à-vis* the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the

possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

(128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

(129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

(130) Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

(131) Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.

(132) Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.

(133) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.

(134) Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.

(135) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

(136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.

(137) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.

(138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.

(140) The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance

with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

(143) Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concerned which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.

Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.

(144) Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first

seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.

(145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.

(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

(147) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council [1] should not prejudice the application of such specific rules.

(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

(150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate

[1] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

(151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

(152) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

(153) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

(154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council ([1]) leaves intact and in no way affects the level of protection of natural persons with regard to the

([1]) Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).

processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.

(155) Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

(156) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

(157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

(158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

(160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

(161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council ([1]) should apply.

(162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

(163) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council ([2]) provides further specifications on statistical confidentiality for European statistics.

(164) As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.

(165) This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.

(166) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement

([1]) Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).

([2]) Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(167) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(168) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.

(169) The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.

(170) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(171) Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.

(172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 ([1]).

(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms *vis-à-vis* the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council ([2]), including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation,

([1]) OJ C 192, 30.6.2012, p. 7.

([2]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

HAVE ADOPTED THIS REGULATION:

*CHAPTER I*

## *General provisions*

*Article 1*

### Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

*Article 2*

### Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

*Article 3*

### Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

*Article 4*

**Definitions**

For the purposes of this Regulation:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the

framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16) 'main establishment' means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(17) 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(18) 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(21) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

(22) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

(23) 'cross-border processing' means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(24) 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(25) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council [1];

(26) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

*CHAPTER II*

## *Principles*

*Article 5*

### Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

[1] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

*Article 6*

**Lawfulness of processing**

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific

processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

*Article 7*

**Conditions for consent**

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

*Article 8*

**Conditions applicable to child's consent in relation to information society services**

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

*Article 9*

**Processing of special categories of personal data**

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

*Article 10*

**Processing of personal data relating to criminal convictions and offences**

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

*Article 11*

**Processing which does not require identification**

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

*CHAPTER III*

***Rights of the data subject***

Section 1

**Transparency and modalities**

*Article 12*

**Transparent information, communication and modalities for the exercise of the rights of the data subject**

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

## Section 2

## Information and access to personal data

### *Article 13*

### Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

*Article 14*

**Information to be provided where personal data have not been obtained from the data subject**

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

*Article 15*

**Right of access by the data subject**

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Section 3

**Rectification and erasure**

*Article 16*

**Right to rectification**

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

*Article 17*

**Right to erasure ('right to be forgotten')**

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

*Article 18*

**Right to restriction of processing**

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

*Article 19*

**Notification obligation regarding rectification or erasure of personal data or restriction of processing**

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

*Article 20*

**Right to data portability**

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Section 4

**Right to object and automated individual decision-making**

*Article 21*

**Right to object**

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

*Article 22*

**Automated individual decision-making, including profiling**

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 5

**Restrictions**

*Article 23*

**Restrictions**

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

*CHAPTER IV*

***Controller and processor***

Section 1

## General obligations

*Article 24*

### Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

*Article 25*

**Data protection by design and by default**

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

*Article 26*

**Joint controllers**

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

*Article 27*

**Representatives of controllers or processors not established in the Union**

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a public authority or body.

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

*Article 28*

**Processor**

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

*Article 29*

**Processing under the authority of the controller or processor**

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

*Article 30*

**Records of processing activities**

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

*Article 31*

**Cooperation with the supervisory authority**

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Section 2

## Security of personal data

*Article 32*

**Security of processing**

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

*Article 33*

**Notification of a personal data breach to the supervisory authority**

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

*Article 34*

**Communication of a personal data breach to the data subject**

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

## Section 3

## Data protection impact assessment and prior consultation

### *Article 35*

### Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

*Article 36*

**Prior consultation**

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the data protection officer;

(e) the data protection impact assessment provided for in Article 35; and

(f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Section 4

## Data protection officer

*Article 37*

### Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

*Article 38*

### Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

*Article 39*

**Tasks of the data protection officer**

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 5

**Codes of conduct and certification**

*Article 40*

**Codes of conduct**

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

*Article 41*

**Monitoring of approved codes of conduct**

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

*Article 42*

**Certification**

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

*Article 43*

**Certification bodies**

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

(a) the supervisory authority which is competent pursuant to Article 55 or 56;

(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council [1] in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

[1] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

*CHAPTER V*

## *Transfers of personal data to third countries or international organisations*

*Article 44*

### General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

*Article 45*

**Transfers on the basis of an adequacy decision**

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

*Article 46*

**Transfers subject to appropriate safeguards**

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

*Article 47*

**Binding corporate rules**

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

*Article 48*

**Transfers or disclosures not authorised by Union law**

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

*Article 49*

**Derogations for specific situations**

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

*Article 50*

**International cooperation for the protection of personal data**

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

*CHAPTER VI*

***Independent supervisory authorities***

Section 1

**Independent status**

*Article 51*

**Supervisory authority**

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

*Article 52*

**Independence**

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

*Article 53*

**General conditions for the members of the supervisory authority**

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

— their parliament;

— their government;

— their head of State; or

— an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

*Article 54*

**Rules on the establishment of the supervisory authority**

1. Each Member State shall provide by law for all of the following:

(a) the establishment of each supervisory authority;

(b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

(c) the rules and procedures for the appointment of the member or members of each supervisory authority;

(d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

(f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

## Section 2

## **Competence, tasks and powers**

### *Article 55*

### **Competence**

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

### *Article 56*

### **Competence of the lead supervisory authority**

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

*Article 57*

**Tasks**

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;

(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

*Article 58*

**Powers**

1. Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

*Article 59*

**Activity reports**

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

*CHAPTER VII*

***Cooperation and consistency***

Section 1

## Cooperation

*Article 60*

### Cooperation between the lead supervisory authority and the other supervisory authorities concerned

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

*Article 61*

**Mutual assistance**

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

*Article 62*

**Joint operations of supervisory authorities**

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

6. Without prejudice to the exercise of its rights *vis-à-vis* third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Section 2

## Consistency

*Article 63*

### Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

*Article 64*

### Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

(a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);

(b) concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

(c) aims to approve the criteria for accreditation of a body pursuant to Article 41(3) or a certification body pursuant to Article 43(3);

(d) aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);

(e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or

(f) aims to approve binding corporate rules within the meaning of Article 47.

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

5. The Chair of the Board shall, without undue, delay inform by electronic means:

(a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and

(b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

7. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.

8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

*Article 65*

**Dispute resolution by the Board**

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

*Article 66*

**Urgency procedure**

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

*Article 67*

**Exchange of information**

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Section 3

## European data protection board

*Article 68*

**European Data Protection Board**

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.

2. The Board shall be represented by its Chair.

3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.

5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

*Article 69*

**Independence**

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

*Article 70*

**Tasks of the Board**

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

(a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;

(b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

(d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);

(e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);

(g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).

(i) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

(j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

(k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;

(l) review the practical application of the guidelines, recommendations and best practices referred to in points (e) and (f);

(m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

(n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

(o) carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);

(p) specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;

(q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

(r) provide the Commission with an opinion on the icons referred to in Article 12(7);

(s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

(t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;

(u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

(x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and

(y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

*Article 71*

**Reports**

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

*Article 72*

**Procedure**

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

*Article 73*

**Chair**

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.

2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

*Article 74*

**Tasks of the Chair**

1. The Chair shall have the following tasks:

(a) to convene the meetings of the Board and prepare its agenda;

(b) to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;

(c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.

2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

*Article 75*

**Secretariat**

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.

3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.

4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.

5. The secretariat shall provide analytical, administrative and logistical support to the Board.

6. The secretariat shall be responsible in particular for:

(a) the day-to-day business of the Board;

(b) communication between the members of the Board, its Chair and the Commission;

(c) communication with other institutions and the public;

(d) the use of electronic means for the internal and external communication;

(e) the translation of relevant information;

(f) the preparation and follow-up of the meetings of the Board;

(g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

*Article 76*

**Confidentiality**

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council ([1]).

*CHAPTER VIII*

***Remedies, liability and penalties***

*Article 77*

**Right to lodge a complaint with a supervisory authority**

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

*Article 78*

**Right to an effective judicial remedy against a supervisory authority**

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

*Article 79*

**Right to an effective judicial remedy against a controller or processor**

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

([1]) Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

*Article 80*

**Representation of data subjects**

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

*Article 81*

**Suspension of proceedings**

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

*Article 82*

**Right to compensation and liability**

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

*Article 83*

**General conditions for imposing administrative fines**

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

*Article 84*

**Penalties**

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

*CHAPTER IX*

***Provisions relating to specific processing situations***

*Article 85*

**Processing and freedom of expression and information**

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

*Article 86*

**Processing and public access to official documents**

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

*Article 87*

**Processing of the national identification number**

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

*Article 88*

**Processing in the context of employment**

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

*Article 89*

**Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in

order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

*Article 90*

**Obligations of secrecy**

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

*Article 91*

**Existing data protection rules of churches and religious associations**

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

*CHAPTER X*

***Delegated acts and implementing acts***

*Article 92*

**Exercise of the delegation**

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.

3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

*Article 93*

**Committee procedure**

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

*CHAPTER XI*

***Final provisions***

*Article 94*

**Repeal of Directive 95/46/EC**

1. Directive 95/46/EC is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

*Article 95*

**Relationship with Directive 2002/58/EC**

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

*Article 96*

**Relationship with previously concluded Agreements**

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

*Article 97*

**Commission reports**

1. By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:

(a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;

(b) Chapter VII on cooperation and consistency.

3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.

4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.

5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

*Article 98*

**Review of other Union legal acts on data protection**

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

*Article 99*

**Entry into force and application**

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from 25 May 2018.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 27 April 2016.

| *For the European Parliament* | *For the Council* |
| --- | --- |
| *The President* | *The President* |
| M. SCHULZ | J.A. HENNIS-PLASSCHAERT |