Impact of the European General Data Protection Regulation on U.S. M&A

March 26, 2018

The winds of change will shortly sweep across the data privacy landscape in the European Union ("**E.U.**") and the gale will be felt worldwide. The European General Data Protection Regulation ("**GDPR**") will come into force on May 25, 2018.[1] Currently, some U.S. M&A practitioners prioritize U.S. law, absent a target with a strong business nexus with the E.U., but the GDPR's extraterritorial scope, together with increased fines for non-compliance (up to the greater of 20,000,000 Euros or four percent of annual global revenue), will force its consideration into U.S. M&A activity.

We discuss below the transactional considerations for investors, purchasers and sellers of U.S. companies arising from the GDPR.

Executive Summary

- The extended jurisdiction of the GDPR will encompass companies, regardless of domicile, that process the personal data related to the offering of goods or services to data subjects in the E.U.
- The risk of substantial fines based on global revenue will increase the importance of conducting thorough due diligence on a target's compliance with data protection laws.
- Transaction structuring and risk allocation mechanisms should expressly contemplate data protection to ensure compliance, and allocate the risk of non-compliance, with the GDPR.
- Monitor GDPR enforcement action and interpretative guidance as implementation clarifies best practices.

Diligence Considerations: GDPR Scope, Compliance and Penalties

Purchasers and investors should first consider whether the target's data processing is subject to the GDPR. Under the GDPR, processing of personal data is defined broadly to include nearly any act that is performed on personal data, including collection, organization, storage, use, and even the destruction of personal data.[2] The GDPR covers processing of personal data that (i) occurs in the context of the activities of an establishment in the E.U.,[3] (ii) is related to the offering of goods or services, regardless of whether payment is required, to individuals in the E.U.,[4] or (iii) is related to the monitoring of individuals'

[1] *EU General Data Protection Regulation*: 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), OJ 2016 L 119/1.

[2] *Id.* Art. 4(2).

[3] *Id.* Art. 3(1). "Establishment" as used in the GDPR will be found when there is effective and real exercise of activity through stable arrangements. *Id.* Recital 22. The legal form of those arrangements, whether as a branch or a corporate entity, is not determinative. *Id.*

[4] *Id.* Art. 3(2)(a).

behavior in the E.U.[5] The "offering of goods or services" may be broadly construed and depends on "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 [European] Union."[6] As a result, the GDPR may apply to U.S. companies that do not have substantial E.U. activities and have not previously focused on E.U. data privacy laws.

- Practice Tip: Do not rely on the target's explanation that they do not have material E.U. operations. Go beyond diligence questions and investigate the company's online presence, including whether visitors to the target's website from the E.U. are provided with local language or shipping options.
- Practice Tip: If the target appears to be subject to the GDPR, consider whether the purchaser will have access to personal data as part of diligence or in the data room. If so, the purchaser could be subject to the GDPR as well and NDAs may need to be tailored accordingly. Unless necessary, some purchasers may prefer to affirmatively exclude any personal data from the data room or diligence process to avoid being subject to the GDPR.
- Practice Tip: For sellers, anticipate purchaser GDPR questions and consider practicing diligence responses with outside counsel to prepare for calls. Given the uncertainties regarding interpretation and enforcement, perfect confidence in GDPR compliance is unlikely to be expected, but being able to conversantly discuss the topics will give purchasers comfort that the issue is being thoughtfully considered.

To the extent that a company may be subject to the GDPR, a purchaser may need to re-evaluate and re-orient the target's data processing activities after the transaction. Such review may look into the process by which the company obtains "freely given, specific, informed and unambiguous"[7] consent from individuals, the company's use of the data and whether it is consistent with the GDPR's data processing principles,[8] and the support of data subjects' rights (including the right to access, rectification, erasure—the "right to be forgotten"—and portability).[9] Under the GDPR, companies must maintain records of their processing activities, including the purposes of the processing, a description of the categories of data subjects and personal data, the categories of recipients, duration of processing, third country transfers and general descriptions of the applicable technical and organizational security measures.[10]

- Practice Tip: The target's records of processing activities will often be a good starting point to approach the key questions, including: (i) Whose personal data is being processed? (ii) What kind of personal data is being processed? (iii) For what purpose? (iv) For how long? (v) Is data transferred to other parties? (vi) Is data transferred out of the E.U.? and (vii) What security measures are in place?

Careful diligence should be conducted on the target's contracts with third parties that are processing data on its behalf, as amendments may be necessary to conform to the GDPR's requirements that such contracts contain specific provisions relating to the processing of personal data.[11] Under the GDPR,

---

[5] *Id*. Art. 3(2)(b).

[6] *Id*. Recital 23.

[7] *Id*. Arts. 4(11) and 7.

[8] *Id*. Art. 5.

[9] *Id*. Arts. 12 and 15-20.

[10] *Id*. Art. 30(1)-(2).

[11] *Id.* Art. 28(3).

transfer of personal data outside the E.U. may typically only be made to countries where the European Commission has determined that the country has an adequate level of protection for personal data.[12] Absent such an adequacy determination (and the U.S. has not been deemed adequate), transfers may only be made on the basis of (i) implementation of appropriate safeguards[13] or (ii) enumerated derogations.[14] Diligence should be conducted with a focus on the existence of such transfers of data outside the E.U. (which, in the case of a U.S. target, may be likely absent local servers) and the applicable justifications for such transfers.

In addition to heightened obligations regarding the processing of personal data, the GDPR also imposes an affirmative requirement for companies to implement appropriate technical and organizational measures to ensure a level of data security appropriate to the risks presented by the nature, scope, context and purposes of the company's data processing and to ensure such measures are taken by a company's third party processors as well.[15]

The GDPR also institutes the strictest data breach notification obligations of any generally applicable cybersecurity law. Companies must notify their "competent supervisory authority" "without undue delay and, where feasible, not later than 72 hours" after becoming aware of a data breach.[16] For particularly egregious breaches, a company may also be required to notify the affected individuals.[17] Whether notification is required or not, the company is required to maintain a breach register and document all breaches—the related facts, effects and remedial action taken—subject to verification by the supervisory authority.[18] During diligence, requesting a copy of the target's breach documentation may be prudent. If the target does not maintain a record of breaches then it may be operating in violation of applicable law and further diligence may be required to identify whether the target has suffered data breaches that may present future regulatory or litigation risk. Breach-related documentation may also be scrutinized for insight into the target's data breach remediation procedures and approach to risk management and compliance.

Depending on the extent of the company's utilization of personal data, compliance with these operational, contractual, governance and notification obligations may prove costly, time-consuming and require C-suite attention.

- Practice Tip: GDPR compliance will not be satisfied—or properly diligenced—by a check-the-box approach. Request a copy of the company's latest data map. The company will need to be able to provide it to a regulator on short notice and if they do not have one ready it may be a sign of an overall lax approach towards compliance.
- Practice Tip: U.S. companies may benefit from building direct relationships, typically through their data protection officer, with appropriate data protection authorities in the E.U. to facilitate a smoother notification process as a single data breach may trigger notification obligations in the U.S. as well as the E.U.

---

[12] *Id.* Art. 45(1).

[13] *Id.* Art. 46.

[14] *Id.* Art. 49.

[15] *Id.* Art. 32(1).

[16] *Id.* Art. 33(1).

[17] *Id.* Art. 34(1).

[18] *Id.* Art. 33(5).

- Practice Tip: For Sellers, pre-empt onerous document requests by proactively providing high-level summaries of the target's personal data practices.

Non-compliance with the GDPR presents a serious risk. Relevant data authorities are empowered under the GDPR with broad investigatory and corrective powers.[19] These include the power to compel companies to provide whatever information may be required to evaluate compliance with the GDPR and conduct data protection audits, including obtaining access to a company's premises.[20] The corrective powers include injunctive relief (including modifying a company's data processing processes, forcing a company to provide notice of a data breach to a data subject or imposing a temporary or permanent ban on data processing) and the ability to impose administrative fines.[21] Administrative fines under the GDPR are not merely compensatory for loss suffered by a data subject, but are rather structured to be "effective, proportionate and dissuasive."[22] The GDPR provides limits to the administrative fines of up to the greater of 20,000,000 Euros or four percent of global annual revenue for violations of core substantive requirements (including with respect to the GDPR's principles for processing, conditions for consent, data subject's rights, and transfers of data).[23] For more procedural violations, there is a lower threshold of the greater of 10,000,000 Euros or two percent of global annual turnover.[24]

Determination of the applicable fine involves a broad, multi-factored evaluation of the nature, gravity and duration of the breach, the intentional or negligent character of the breach, any attempts at mitigating harm and how the relevant data authority became aware of the breach (e.g., whether the company itself notified the data authority).[25] The data authorities in the E.U. will be able to enforce directly against assets in the E.U., but there are contemplated discussions between the European Commission, the FTC and Department of Commerce regarding further cooperation on enforcement.[26]

With the nearing implementation of the GDPR, business and legal communities are anxiously awaiting the first few enforcement actions to judge how and at what level these administrative fines will be levied.

- Practice Tip: Investigate the company's history of cooperation with data privacy regulators in the E.U., and its past handling of data breaches. A history of regulator cooperation may help mitigate future fines.
- Practice Tip: Carefully probe the company's personal data retention practices with an eye towards confirming that the company only retains personal data as necessary.

Valuation Considerations

Should the GDPR apply, consider (i) how consistent the valuation model is with the scope of the company's ability to use its personal data, (ii) the potential costs to bring the business into compliance

---

[19] *Id*. Art. 58.

[20] *Id*. Art. 58(1).

[21] *Id*. Art. 58(2).

[22] *Id*. Art. 83(1).

[23] *Id*. Art. 83(5).

[24] *Id*. Art. 83(4).

[25] *Id. A*rt. 83(2).

[26] *See* E.U.-U.S. Privacy Shield – First annual Joint Review, Article 29 Data Protection Working Party, adopted on Nov. 28, 2017. For additional context, the FTC brought its own enforcement actions against U.S. companies that have falsely claimed benefit of the E.U.-U.S. Privacy Shield Framework. **https://www.ftc.gov/news-events/press-releases/2017/09/three-companies-agree-settle-ftc-charges-they-falsely-claimed** (last accessed Mar. 23, 2018).

with the GDPR from an operational, contractual and governance perspective, and (iii) reputational and financial risks associated with GDPR non-compliance.

One of the GDPR's core principles is the purpose limitation, which binds companies to the specified, explicit and legitimate purposes communicated to the data subject when their personal data is collected.[27] Further processing beyond the original communicated purposes is allowed only to the extent that such processing is not incompatible with the original purpose.[28] If the purchaser's valuation model relies on different or expanded use of the target's database of personal data, a purchaser may need to communicate a new privacy statement to each data subject and, in certain instances, obtain affirmative consent in order to be compliant.[29] The cost and time associated with this exercise may impact the purchaser's business plan as the GDPR may require affirmative consents that may not be satisfied by, for example, simply updating a privacy policy on a website.

- Practice Tip: Push financial modelers on their models and assumptions and communicate personal data-related assumptions to legal and business teams to focus on during diligence.
- Practice Tip: For Sellers, update privacy policies or obtain appropriate consent before the transaction to ensure that the company's database of personal data may be transferred in connection with a merger or similar transaction.

The implementation of certain operational, governance and contractual measures prescribed by the GDPR, including those described above, may impose additional financial costs. For instance, in a scenario where the acquisition expands the data processing activities of the target to constitute large scale, regular and systematic monitoring of data subjects, the appointment of a data protection officer may be required.[30] The company may also need to implement extensive documentation processes[31] and conduct data protection impact assessments.[32] This would be in addition to amending its existing contractual arrangements with third parties (which beyond the diversion of resources may require additional consideration)[33] and the implementation of appropriate data protection measures.[34] The total costs of such measures could be significant.

- Practice Tip: The diligence gap analysis should include a review of technical cybersecurity and physical security operations as well as an appreciation of the headcount of the company's data privacy compliance function. IT upgrades can be a significant expense and, if the compliance function is understaffed, additional resources may be required.

Non-compliance with the GDPR risks severe financial and reputational harm. As discussed above, administrative fines for non-compliance can be punitive and the indirect costs of dealing with a data breach can also be significant, involving third-party costs of investigation and remediation (and may involve notifications and credit monitoring, where applicable). Reputational harm associated with a data breach can be even more problematic for companies that rely heavily on consumer trust.

---

[27] *Id*. Art. 5(1)(b).

[28] *Id*.

[29] *Id.*

[30] *Id.* Art. 37(1).

[31] *Id.* Art. 30(1).

[32] *Id.* Art 35.

[33] *Id.* Art. 28(3).

[34] *Id*. Art. 32(1).

- Practice Tip: Nearly every company faces actual or attempted data security breaches with regularity. The more important question is whether the target company is aware of these attempts and taking measures to ensure its data is as secure as reasonably possible. Do not limit diligence to the target's legal staff; also speak with the Chief Information Officer regarding penetration testing, patch and logging procedures, and the target's information security and breach response plans.
- Practice Tip: For Sellers, if the company has a history of data breaches, carefully summarize the scope of the breaches, the company's responses and any material impacts on the business.

Purchase Agreement Considerations

Prudent purchasers and investors will factor GDPR compliance into their purchase agreement structuring and risk allocation mechanisms. If the transaction is structured as an asset purchase, particular care will be needed to determine whether the transfer of the target's databases itself may violate the GDPR (e.g., by exceeding the scope of the applicable consent or by transferring data outside of the E.U. to a jurisdiction that has not been deemed adequate by the European Commission).[35] Covenants may be appropriate to ensure continued compliance (or development of a compliance program) or notification of any new breaches between signing and closing the transaction. Risk allocation provisions should also be thoughtfully negotiated to ensure appropriate excluded liability, representation and indemnity coverage. Representations regarding compliance with law are insufficient to fully address data privacy risks and should be expanded to cover data-privacy related contract provisions, industry standards and practices, and existence and handling of data breaches. Representations to consider also include: (i) operation in accordance with the company's written privacy policy, (ii) provision of all applicable privacy and cybersecurity policies, (iii) absence of written notices regarding related investigations, (iv) existence of commercially reasonable information security program, (v) absence of restrictions with respect to target's successors' rights to use, sell, license, distribute, and disclose personal data, and (vi) absence of data security breaches, loss of data, and unauthorized disclosures of personal sensitive information.

- Practice Tip: In an asset deal, consider making GDPR non-compliance an excluded liability. Include not only pre-closing operations, but also a reasonable period of time post-closing so that the purchaser has a covered window to bring the business into compliance.
- Practice Tip: Depending on the duration between signing and closing, consider adding a covenant for the target to bring itself into compliance with the GDPR before closing. Purchasers that are operating companies with their own robust privacy programs may instead prefer to simply onboard the target as part of post-closing integration.
- Practice Tip: To the extent possible as part of the larger deal dynamic, indemnities backing the related representations should be uncapped or subject to limitations of liability sufficiently high to cover the GDPR's global revenue-based fines.
- Practice Tip: If a purchaser is planning to rely on representation and warranty insurance, ensure that data privacy is not on the list of exclusions and carefully discuss with outside counsel the extent to which data privacy diligence should be conducted (as known liabilities are typically excluded from the scope of coverage, regardless of whether they are ultimately disclosed as part of the transaction agreement). Also keep in mind that representation and

[35] As transfers of data to jurisdictions that have not been deemed adequate by the European Commission are prohibited unless those transfers are made subject to other specified appropriate safeguards or derogations. *Id.* Arts. 45(1), 46 and 49.

warranty insurance, which is often capped at 10% of purchase price, may be insufficient to cover fines under the GDPR.

Post-Transaction Considerations

The post-closing process of transferring and integrating data can last for up to several years, especially if the acquisition involves a business carve-out with related transitional services arrangements. During this period, either the seller or the purchaser may be required to continue data processing for the other. In these cases, the GDPR will require the incorporation of specific contractual provisions between the parties in the applicable transitional services agreement.

After the transaction, the purchaser may want to consolidate the target's data at the purchaser's existing data centers. If such transfers involve the movement of data outside the E.U., specific measures must be complied with if the recipient country has not been deemed adequate with respect to the protection of personal data by the European Commission.[36] The U.S. has not been deemed adequate and so transfers may only be made subject to appropriate safeguards[37] or enumerated derogations.[38] The current most viable option for broadly permitting transfers to the U.S. may be the E.U.-U.S. Privacy Shield Framework that received an adequacy decision from the European Commission.[39] Under this framework, companies may self-certify compliance with certain requirements and submit such certification to the U.S. Department of Commerce to benefit from the adequacy decision. However, the continued viability of this framework is uncertain given significant concerns regarding the U.S. government's national security personal data practices. As an alternative solution, affiliates may consider implementing binding corporate rules to implement appropriate safeguards for intra-group data transfers.[40] Consideration should also be given as to how the affected data subjects would be informed of (and have an opportunity to object to) the movement of their personal data outside the E.U.

Conclusion

The GDPR becomes effective on May 25, 2018, and prudent purchasers and sellers are already working with their counsel to better understand a company's evolving data privacy risk profile under the GDPR and how best to allocate such risks in the transactional setting. The implications of the GDPR may impact all phases of a deal and should be taken into consideration from diligence through structuring to post-closing integration activities. We will monitor and provide further updates as the GDPR becomes effective and enforcement actions begin.

---

[36] *Id.* Art. 45(1).

[37] *Id*. Art. 46.

[38] *Id.* Art. 49.

[39] For more information, *see* https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en (last accessed Mar. 23, 2018).

[40] *Id*. Art. 47.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

Frank Azzopardi	**+1 (212) 450-6277**	**frank.azzopardi@davispolk.com**
Leo Borchardt	**+44 (20) 7418 1334**	**leo.borchardt@davispolk.com**
Avi Gesser	**+1 (212) 450-4181**	**avi.gesser@davispolk.com**
Pritesh Shah	**+1 (212) 450-4147**	**pritesh.shah@davispolk.com**
Michelle Ontiveros Gross	**+1 (650) 752-2073**	**michelle.gross@davispolk.com**
Daniel Forester	**+1 (212) 450-3072**	**daniel.forester@davispolk.com**

© 2018 Davis Polk & Wardwell LLP | 450 Lexington Avenue | New York, NY 10017

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's **privacy policy** for further details.