ANNEX

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council
ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause I

Purpose and scope

(a) The purpose of these standard contractual clauses (the Clauses) is to ensure compliance with the requirements of 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 (General Data Protection Regulation)\footnote{Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to the Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the Standard Contractual Clauses included in Decision […].} for the transfer of personal data to a third country.

(b) The Parties:

8.1 the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and

8.2 the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via an intermediary another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”).

have agreed to these standard data protection contractual clauses (hereinafter: “Clauses”).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

9 These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1), and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 46(2)(d).
Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to

\[1\] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].
This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract, and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the standard contractual clauses these Clauses or prejudice the fundamental rights or freedoms of data subjects.

These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of the Regulation (EU) 2016/679.

(d) These Clauses apply with respect to the transfer of personal data as specified in Clause 5 of Section I [Description of the Transfer(s)].

(e) Annexes I, II and III form an integral part of these Clauses.

Clause 2

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Section I;

(ii) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(iii) Clause 8 - Module One: Clause 1.5, and Clause 1.9(b);

Module Two: Clause 1.9(b), 8.9(a), (c), (d) and (e); Module Three: Clause 1.8.1(a), (c) and (d) and Clause 1.9.9(a), (c), (d) and (e), (f) and (g); Module Four: Clause 1.1, Clause 2.8.1(b) and Clause 4.3.8.3(b);

(iv) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iii) Section II, Clause 3.1(c), (d) and (e); Module Two and Three: Clause 7.12(a), (b) and (d); Modules Two and Three: Clause 7.12(a), (b) and (f);

(v) Clause 15.1(c), (d) and (e);

(vi) Section II, Clause 9.16(e);

(vii) Clause 18 - Modules One, Two and Three: Clause 3.18(a), (b) and (e); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 3

Interpretation

(a) Where these Clauses use the terms that are defined in Regulation (EU) 2016/679,
those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.
**Clause 4**

_Hierarchy_

In the event of a **conflict** between these Clauses and the provisions of any other related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

---

**Clause 5**

_Description of the transfer(s)_

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B [Description of the transfer(s)].

---

**Clause 6 - Optional**

_Docking clause_

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing Annex I.A [List of Parties], Annex I.B [Description of the transfer(s)] and Annex II [Technical and organisational measures] the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding Party entity shall have no rights or obligations arising under these Clauses from the period prior to the date of signing Annex I.A becoming a Party.

---

**SECTION II – OBLIGATIONS OF THE PARTIES**

**Clause 1**

_Data protection safeguards_

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

---

**MODULE ONE: Transfer controller to controller**

• **1.1 Purpose limitation**

The data importer shall not process the personal data only for any purposes that are incompatible with the specific purpose(s) of the transfer, as set out in Annex I.B. [Description of the transfer(s)], unless it has obtained the data subject’s prior consent. **It may only process the personal data for another purpose:**
(i) where it has obtained the data subject’s prior consent;
(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.
1.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 5 of Section II, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;
(ii) where it intends to process the personal data received from the data exporter for a different purpose than the purpose(s) of the transfer pursuant to Annex I.B. [Description of the transfer(s)], of that different purpose;

(iii) of the categories of personal data processed;

(iv) of the right to obtain a copy of these Clauses;

(v) where it intends to disclose onward transfer the personal data to any third party/ies, of the identity of that third party and recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such disclosure onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing such information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) The parties shall provide a copy of these Clauses, including the Appendix as completed by them, available to the data subject upon request free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Annexes to these Clauses prior to sharing a copy, but shall provide a meaningful summary where otherwise the data subject would otherwise not be able to understand the content of the Annexes to these Clauses. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Subparagraphs (a) to (c) are notwithstanding without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679, in particular to inform the data subject about the transfer of special categories of data.

1.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date, to the extent necessary having regard to the purpose(s) of processing. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(e) The data importer shall ensure that the personal data is adequate, relevant and
limited to what is necessary in relation to the purpose(s) of processing.

- **1.4 Storage limitation**
  The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures
to ensure compliance with this obligation, including erasure or anonymisation\(^2\) of the data and all of its back-ups at the end of the retention period.

\*\*\* 1.5. Security of processing \*\*\*

(a) The data importer and, during the transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the risks involved in the processing, state of the art, the costs of implementation, the nature of the personal data and the nature, scope, context and purpose(s) of processing, and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, and anonymisation or pseudonymisation where this does not prevent fulfilling, where the purpose of processing, can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) If a personal data breach that is likely to result in significant adverse effects a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority within the meaning of Clause 9 of Section II [Supervision] pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the data breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In addition, in such cases in case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also, if necessary in cooperation with the data exporter, notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in subparagraph c), paragraph (e), points ii) to iv), unless this the data importer has

---

\(^2\)In line with recital 26 of the Regulation (EU) 2016/679, this requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, and that this process is irreversible.
implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

---

2 This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.
The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

1.6. **Special categories of personal data**

- **Sensitive data**

To the extent the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter “special categories of sensitive data”), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and additional restrictions with respect to further disclosure.

- **1.7. Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) unless the third party is or agrees to be bound by these Clauses. Alternatively, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

  (i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

  (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

  (iii) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 Regulation (EU) 2016/679 that covers the onward transfer;

  (iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

  (v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

  (vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of the purpose(s) of the onward transfer, the identity of recipient(s) or categories of recipients, the recipient and of the possible risks of such transfer to the data subject due to the lack of appropriate

---

1 The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States: Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereof. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.
data protection safeguards for the onward transfer. In this case, the data importer shall inform the data exporter and, at the request of the data exporter, shall provide a copy of the information provided to the data subject.

3 The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.
Any disclosure may only take place subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

- **1.8** Processing under the authority of the data importer
  The data importer shall ensure that any person acting under its authority, including a processor, does not process the data except on instructions from the data importer.

- **1.9** Documentation and compliance
  8. (a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
  9. (b) The data importer shall make such documentation available to the competent supervisory authority on request.

**MODULE TWO: Transfer controller to processor**

- **1.1** Instructions
  (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give further instructions regarding the data processing, within the framework of the contract agreed with the data importer, throughout the duration of the contract, but such instructions shall always be documented.
  (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

- **1.2** Purpose limitation
  The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B (Description of the transfer(s)), unless on further instructions from the data exporter.

- **1.3** Transparency
  The data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject with a copy of the Clauses upon request free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the Parties may redact part of the text of the Annexes that is otherwise not be able to understand the content of the Annexes. This is notwithstanding or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679, in particular to inform the data subject about...
the transfer of special categories of data.

- **1.4 Accuracy**

If one of the Parties\_\text{data importer} becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other \text{Parties\_data exporter} without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.
1.5 Storage limitation and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. Upon termination of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. This is notwithstanding any requirements under local law. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer prohibiting return or deletion of the personal data, the data importer shall warrant that it will guarantee, to the extent possible, the level of protection required by these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

1.6 Security of processing

(a) The data importer and, during the transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the risks involved in the processing, state of the art, the costs of implementation, the nature of the personal data and the nature, scope, context and purpose(s) of processing, and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission—and anonymisation or pseudonymisation where this does not prevent fulfilling, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact...
point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to **be taken** address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all
information at the same time, the initial notification shall contain the information then available and further information shall be provided subsequently as it becomes available, subsequently be provided without undue delay.

13 (d) The data importer shall cooperate in good faith with and assist the data exporter in any way necessary to enable the data exporter to comply with its obligations under the Regulation (EU) 2016/679, notably in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

1.7 Special categories of personal data

• Sensitive data

To the extent the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “special categories of sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B [Description of the transfer(s)].

• 1.8 Onward transfers

The data importer shall only disclose the personal data to a third party on the basis of documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses or, alternatively, an onward transfer by the data importer may only take place under the appropriate Module, or if:

• the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

• the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

• the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

• the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 Regulation (EU) 2016/679 that covers the onward transfer necessary in order to protect the vital interests of the data subject or of another natural person.

Any disclosure may only take place onward transfer is subject to compliance by the data

---

The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States: Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereof. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.
importer with all the other safeguards under these Clauses, in particular purpose limitation.

4 The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.
• **1.9. Documentation and compliance**

8 (a) The data importer shall promptly and **properly**, **adequately** deal with enquiries from the data exporter that relate to the processing under these Clauses.

9 (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter under its responsibility.

10 (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to reviews of data files and documentation, or of audits of the processing activities covered by these Clauses, in particular at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

11 (d) The data exporter may choose to conduct the audit by itself, to mandate, at its own cost, an independent auditor or to rely on an independent audit mandated by the data importer. Where the data importer mandates an audit, it has to bear the costs of the or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

12 (e) The data importer Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

**MODULE THREE: Transfer processor to processor**

• **1.1. Instructions**

(a) (a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s) as specified in Annex I.A. [List of parties], which the data exporter shall make available to the data importer prior to processing.

(b) (b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing within the framework of the contract agreed with the data importer throughout the duration of the contract, but such instructions shall always be documented.

(c) (c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. To Where the extent the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller thereof.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.
See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.
• **1.2** Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. [Description of the transfer(s)], unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

• **1.3** Transparency

The data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject upon request free of charge. To the extent necessary to protect business secrets or other confidential information, the Parties, including personal data, the data exporter may redact part of the text of the Annexes to these Clauses Appendix prior to sharing a copy, but shall provide a meaningful summary where otherwise the data subject would otherwise not be able to understand the content of the Annexes or its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

• **1.4** Accuracy

If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party, and the controller, without undue delay. In this case, the data importer shall cooperate with the data exporter and the controller to rectify or erase the data.

• **1.5** Storage limitation

Processing by the data importer shall only take place for the duration specified in Annex I.B. Upon termination of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so. If the data importer or data exporter return to the data exporter all personal data processed on its behalf and delete existing copies. This is notwithstanding any requirements under local law. If the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer prohibiting return or destruction of the personal data, the data importer shall warrant that it will guarantee, to the extent possible, the level of protection required by continuing to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

• **1.6** Security of processing

(a) The data importer and, during the transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data.
(hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the risks involved in the processing, state of the art, the costs of implementation, the nature of the personal data and the nature, scope, context and purposes purpose(s) of processing, and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission and anonymisation or pseudonymisation where this does not prevent fulfilling, where the purpose of processing
can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this obligation paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II—[Technical and organisational measures]. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall be provided subsequently as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate in good faith with and assist the data exporter in any way necessary to enable the data exporter to comply with its obligations under the GDPR, notably Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

1.7 Special categories of personal data

- Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter “special categories of sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B—[Description of the transfer(s)].

- 1.8 Onward transfers

The data importer shall only disclose the personal data to a third party on the basis of documented instructions from the controller as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the
The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereof. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.
(in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses or, alternatively, an onward transfer by the data importer may only take place under the appropriate Module, or if:

- the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

- the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 GDPR of Regulation (EU) 2016/679;

- the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

- the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 GDPR that covers the onward transfer necessary in order to protect the vital interests of the data subject or of another natural person.

Any disclosure may only take place if the onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

- 1.9 Documentation and compliance

  (a) The data importer shall promptly and properly deal with inquiries from the data exporter or the controller that relate to the processing under these Clauses.

  (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities on behalf of the controller under its responsibility.

  (c) The data importer shall make available to the data exporter and the controller all information necessary to demonstrate compliance with the obligations set out in these Clauses and available to the data exporter, which shall provide it to the controller.

  (d) The data importer shall allow for and contribute to reviews of data files and documentation, or to audits of the data exporter of the processing activities covered by these Clauses, in particular at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on a review or an audit, the controller or data exporter may take into account relevant certifications held by the data importer.

  (e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

  (f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

  (g) The data importer Parties shall make the information referred to in paragraphs (b)
and (c), including the results of any audits, available to the competent supervisory authority on request.

data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.
MODULE FOUR: Transfer processor to controller

(i) 1.1 Instructions

(b) (a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(c) (b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe the GDPR Regulation (EU) 2016/679 or other Union or Member State data protection law.

(d) (c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under the GDPR Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(e) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

(ii) 1.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during the transmission, and the protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the risks involved in the processing, the costs of implementation, the nature of the personal data and the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, anonymisation or pseudonymisation where this does not prevent fulfilling, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(ii) 1.3 Documentation and compliance

---

*This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences.
(a) The Parties shall be able to demonstrate compliance with these Clauses.

This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences.
(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 29

Local laws affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (only if the EU processor combines the personal data received from the third country controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the Clauses.

(b) The Parties declare that in providing the warranty in paragraph a, they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing; the nature of the personal data transferred; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred;

(ii) the laws of the third country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities, as well as the applicable limitations and safeguards;

(iii) any safeguards in addition to those under these Clauses, including the technical and organisational measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph b), it has made best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
(d) The parties agree to document the assessment under paragraph b) and make it available to the competent supervisory authority upon request.

(e) The data importer agrees to promptly notify the data exporter if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws not in line with the requirements under paragraph a), including following a change of the laws in the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements under paragraph a).

(f) Following a notification pursuant to paragraph e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under the Clauses, the data exporter shall promptly identify appropriate measures (such as, for instance, technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and / or data importer to address the situation, if appropriate in consultation with the [for Module Three: controller and] competent supervisory authority. If the data exporter decides to continue the transfer, based on its assessment that these additional measures will allow the data importer to fulfill its obligations under the Clauses, the data exporter shall forward the notification to the competent supervisory authority together with an explanation, including a description of the measures taken. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall inform the competent supervisory authority and shall be entitled to terminate the contract. In case the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the responsible Party, unless the Parties have agreed otherwise. When the contract is terminated pursuant to this Clause, Section III, Clause 1 (d) and (e) shall apply.

Clause 3

Obligations of the data importer in case of government access requests

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (only if the EU processor combines the personal data received from the third country controller with personal data collected by the processor in the EU)

3.1 Notification

(a) The data importer agrees to promptly notify the data exporter and, where possible, the data subject (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request by a public authority under the laws of the country of destination for disclosure of personal data transferred pursuant to these Clauses; such notification shall include

---

9 This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.
information about the personal data requested, the requesting authority, the legal basis for the request and the response provided;

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicate as much information and as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them upon request of the data exporter.

(c) To the extent permissible under the laws of the country of destination, the data importer agrees to provide to the data exporter, in regular intervals for the duration of the contract, the greatest possible amount of relevant information on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs a) to c) for the duration of the contract and make it available to the competent supervisory authority upon request.

(e) Paragraphs a) to c) are notwithstanding the obligation of the data importer pursuant to Clause 1 of Section III [Termination] to promptly inform the data exporter where it is unable to comply with these Clauses.

3.2 Review of legality and data minimisation

(a) The data importer agrees to review, under the laws of the country of destination, the legality of the request for disclosure, notably whether it remains within the powers granted to the requesting public authority, and to exhaust all available remedies to challenge the request if, after a careful assessment, it concludes that there are grounds under the laws of the country of destination to do so. When challenging a request, the data importer shall seek interim measures with a view to suspend the effects of the request until the court has decided on the merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are notwithstanding the obligations of the data importer pursuant to Clause 2(e) of this Section.

(b) The data importer agrees to document its legal assessment as well as any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make it available to the data exporter. It shall also make it available to the competent supervisory authority upon request.

(e) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

---

1 This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.
Clause 4

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION: The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter’s prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the concerned sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s). The list of sub-processors the data importer intends to engage can be found in Annex III from an agreed list. The data importer shall specifically inform the data exporter in writing of any changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor for specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract which provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Section II, Clause 1.8 [Onward transfers]. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter’s request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor’s obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third party beneficiary clause with the sub-processor whereby, in the event of bankruptcy of the data importer, has factually

---

1 This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.
This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

---

1 This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.
This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

**MODULE THREE: Transfer processor to processor**

(f) **OPTION 1**: **SPECIFIC PRIOR AUTHORISATION**: The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the concerned sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: **GENERAL WRITTEN AUTHORISATION**: The data importer has the controller’s general authorisation for the engagement of sub-processor(s). The list of sub-processors the data importer intends to engage can be found in Annex III from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of such engagement. The Parties shall keep Annex III up to date.

(g) Where the data importer engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a written contract which provides for, in substance, the same data protection obligations as the ones binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.² The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Section II, Clause 1.8 [Onward transfers]. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(h) The data importer shall provide, at the data exporter’s or controller’s request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(i) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor’s obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

¹ This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.
(j) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby, in the event of bankruptcy of the data importer, has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall be a third-party beneficiary to the have the right to terminate the

---

1 This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.
sub-processor contract and shall have the right to enforce the contract against the sub-processor, including where applicable by instructing the sub-processor to erase or return the personal data.

Clause 5.10

Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any inquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay, and at the latest within one month of the receipt of the inquiry or request. The data importer shall take appropriate measures to facilitate such inquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge, without undue delay and at the latest within one month of the receipt of the request:

- (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, provide a copy of the data relating to him/her as well as and the information contained in Annex I, information on, if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with the competent supervisory authority in accordance with Clause 12(c)(i);

- (ii) rectify inaccurate or incomplete data concerning the data subject;

- (iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) Where the data importer intends to make decisions based solely on the automated processing of the personal data transferred without human involvement (hereinafter “automated decisions”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, it shall, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, 7That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.
the data importer shall, where necessary in cooperation with the data exporter:

That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.
• (i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

• (ii) implement suitable safeguards, at least by enabling the data subject to contest the automated decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) GDPR of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and about the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial review.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter about of any inquiry or request it has received directly from a data subject. It shall not respond to that inquiry or request itself unless and until it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

(b) Taking into account the nature of the processing, the data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects’ inquiries and requests for the exercise of their rights under the GDPR.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller about of any inquiry or request it has received directly from a data subject, without responding to that inquiry or request unless and until it has been otherwise-authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the
extent of the assistance required.
(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

(b) Taking into account the nature of the processing, the data importer shall assist the controller in fulfilling its obligations to respond to data subjects’ inquiries and requests for the exercise of their rights.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to inquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under the GDPR Regulation (EU) 2016/679.

Clauses

Redress

(d) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints or requests. It shall promptly deal with any complaints or requests by it receives from a data subject.

[OPTION: The data importer agrees that the data subject subjects may also lodge a complaint with [Insert name of an independent dispute resolution body] at no cost to the data subject. It shall inform the data subject subjects, in the manner set out in paragraph (a), of this additional redress mechanism and that they are not required to make use of such additional redress mechanism, or follow a particular sequence in seeking redress.]
(g) **(e)** The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) GDPR of Regulation (EU) 2016/679.

---

The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.
(d) The data importer accepts to shall abide by a decision that is binding under the applicable EU or Member State law.

(i) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 212

Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any material or non-material damages it causes the other Party/ies by any breach of these Clauses.

(b) Liability as between the Parties is limited to actual damage suffered. Punitive damages are excluded.

(c) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject for any breach of the third party by breaching the third-party beneficiary rights under these Clauses.

(d) Notwithstanding paragraph (d), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material
or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject for any breach of the third-party by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the
data exporter is a processor acting on behalf of a controller, to the liability of the controller under the GDPR Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(i) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(j) Where more than one Party is responsible for any damage caused to the data subject resulting from a breach of these Clauses, both all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against either any of these Parties.

(f) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 8
Indemnification

(k) The Parties agree that if one Party is held jointly and severally liable for a breach of these Clauses together with another Party, it is liable under paragraph (e), it shall be entitled to claim back as indemnification from the other Party/ies that part of the liability that corresponds to the other Party’s part of compensation corresponding to its / their responsibility for the damage.

(l) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 9
Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) (a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with the GDPR Regulation (EU) 2016/679 as regards the data transfer, namely [Specify Supervisory Authority and Member State] as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within]
the territorial scope of application of the GDPR according to Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:

The supervisory authority of one of the Member States in which the data subjects whose personal data are transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, namely [Specify Member State] as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to inquiries.
submit itself to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination— including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards.**

---

12 As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such
requests, covering a sufficiently representative time-frame. This refers in particular to internal records or
(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The Parties agree to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor
practice, such as case law and reports by independent oversight bodies.
A. **Notification**

(b) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

1. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

2. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(c) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(d) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(e) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(f) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

A. **Review of legality and data minimisation**

1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and
principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IIIIV – FINAL PROVISIONS

Clause 116

Non-compliance with the Clauses and termination

1. (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

2. (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is notwithstanding without prejudice to Clause 214(f) of Section II.

3. (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   1. (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

   2. (ii) the data importer is in substantial or persistent breach of these Clauses;

   3. (iii) the data importer fails to comply with a binding decision of a competent court or the competent supervisory authority regarding its obligations under these Clauses.

In this case, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the responsible Party, unless the Parties have agreed otherwise.

4. (d) [For Modules One, Two and Three: Personal data that has already been transferred prior to the termination of the contract pursuant to paragraph (c) shall be returned to the data exporter or destroyed in its entirety. The same shall apply to any copies of the data. For Module]
Four: Personal data
be destroyed in their entirety, including any copy thereof. The data importer shall certify the destruction of the data to the data exporter. These obligations are notwithstanding any requirements under local law. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses.

5. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) the GDPR Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under the GDPR Regulation (EU) 2016/679.

Clause 2

Governing law

OPTION 1: These Clauses shall be governed by the law of one of the EU Member States of the European Union, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _______.

OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State of the European Union where the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _______.

Clause 3

Choice of forum and jurisdiction

OPTION 1: These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _______.

1. Any dispute arising from these Clauses shall be resolved by the courts of an EU
Member State of the European Union. The Parties agree to submit themselves to the jurisdiction of such courts.

2. (b) The Parties agree that those shall be the courts of ____ (specify Member State).
3. (c) Legal proceedings by a data subject may also bring legal proceedings against the data exporter and/or data importer may also be brought before the courts of the Member State where the data subject in which he/she has his/her habitual residence.

4. The Parties agree to submit themselves to the jurisdiction of such courts.

**MODULE FOUR: Transfer processor to controller**

Any dispute arising from these Clauses shall be resolved by the courts of (specify country).
APPENDIX

EXPLANATORY NOTE:
It must be possible to clearly distinguish the information applicable to each transfer or category
of transfers and, in this regard, to determine the respective role(s) of the Parties as data
exporter(s) and/or data importer(s). This does not necessarily require completing and signing
separate appendices for each transfer/category of transfers and/or contractual relationship,
where this transparency can achieved through one appendix. However, where necessary to
ensure sufficient clarity, separate appendices should be used.

ANNEX I

1. A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor
MODULE FOUR: Transfer processor to controller

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable,
of the data exporter’s data protection officer and/or representative in the European Union]

1. Name: …
   Address: …
   Contact person’s name, position and contact details: …
   Activities relevant to the data transferred under these Clauses: …
   Signature and date: …
   Role (controller/processor): …

2. …

Data importer(s): [Identity and contact details of the data importer(s), including any contact
person with responsibility for data protection]

1. Name: …
   Address: …
   Contact person’s name, position and contact details: …
   Activities relevant to the data transferred under these Clauses: …
   Signature and date: …
Role (controller/processor): …

2. …
2. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor
MODULE FOUR: Transfer processor to controller

[For processor to processor transfers: identity and contact details of the controller(s):

1. Name:....
   Address:....
   Contact person’s name, position and contact details:....
   Activities relevant to the transfer:....
   Signature and date:....

2. ....]

B. DESCRIPTION OF THE TRANSFER

[For transfers to (sub-) processors, this annex reflects the corresponding instructions received from the controller(s):

Categories of data subjects whose personal data is transferred

.............................

Categories of personal data transferred

.............................

Special categories of personal Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

.............................

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

.............................

Nature of the processing

.............................

Purpose(s) of the data transfer and further processing

.............................

Maximum data retention periods, if applicable
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing
3. **COMPETENT SUPERVISORY AUTHORITY**

**MODULE ONE:** Transfer controller to controller
**MODULE TWO:** Transfer controller to processor
**MODULE THREE:** Transfer processor to processor

*Identify the competent supervisory authority/ies in accordance with Clause 13*
ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

[For transfers to (sub-)processors, this annex reflects the corresponding instructions received from the controller(s):]

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s), (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[TAKING INTO ACCOUNT THE NATURE, SCOPE, CONTEXT AND PURPOSES OF THE PROCESSING ACTIVITY AS WELL AS THE RISK FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS, DESCRIBE ELEMENTS THAT ARE ESSENTIAL TO THE LEVEL OF SECURITY]

For example [Examples of possible measures:
[DESCRIBE REQUIREMENTS FOR PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA]

[DESCRIBE REQUIREMENTS FOR ENSURING ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES]

[DESCRIBE REQUIREMENTS FOR THE ABILITY TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT]

[DESCRIBE REQUIREMENTS FOR PROCESSES FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES FOR ENSURING THE SECURITY OF THE PROCESSING]

[DESCRIBE REQUIREMENTS FOR USERS IDENTIFICATION AND AUTHORISATION]

[DESCRIBE REQUIREMENTS FOR THE PROTECTION OF DATA DURING TRANSMISSION]

[DESCRIBE REQUIREMENTS FOR THE PROTECTION OF DATA DURING STORAGE]

[DESCRIBE REQUIREMENTS FOR PHYSICAL SECURITY OF LOCATIONS AT WHICH PERSONAL DATA ARE PROCESSED]

[DESCRIBE REQUIREMENTS FOR EVENTS LOGGING]
Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products
Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the data (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:
This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name:...
   Address:...
   Contact person’s name, position and contact details:...
   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):...

2. ...
<table>
<thead>
<tr>
<th>Summary report:</th>
<th>Litera® Change-Pro for Word 10.7.0.7 Document comparison done on 6/4/2021 6:42:04 PM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Style name:</strong></td>
<td>Color Legislative Moves+Images</td>
</tr>
<tr>
<td><strong>Intelligent Table Comparison:</strong></td>
<td>Active</td>
</tr>
<tr>
<td><strong>Original DMS:</strong></td>
<td>iw://DMS/AmericasActive/93857598/1</td>
</tr>
<tr>
<td><strong>Modified DMS:</strong></td>
<td>iw://DMS/AmericasActive/94635673/1</td>
</tr>
<tr>
<td><strong>Changes:</strong></td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>952</td>
</tr>
<tr>
<td>Delete</td>
<td>746</td>
</tr>
<tr>
<td>Move From</td>
<td>152</td>
</tr>
<tr>
<td>Move To</td>
<td>152</td>
</tr>
<tr>
<td>Table Insert</td>
<td>0</td>
</tr>
<tr>
<td>Table Delete</td>
<td>0</td>
</tr>
<tr>
<td>Table moves to</td>
<td>0</td>
</tr>
<tr>
<td>Table moves from</td>
<td>0</td>
</tr>
<tr>
<td>Embedded Graphics (Visio, ChemDraw, Images etc.)</td>
<td>1</td>
</tr>
<tr>
<td>Embedded Excel</td>
<td>0</td>
</tr>
<tr>
<td>Format changes</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total Changes:</strong></td>
<td>2003</td>
</tr>
</tbody>
</table>