STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Transfer controller to processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual 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)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) 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

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

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

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

[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, 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 2021/915.

Commented [A1]: Explanation of colors and comments in this document:

• Please provide/insert the info for the areas marked in yellow. With our additional comments in this document, we want to provide further background.

(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

(a) 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 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. 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, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

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

(ii) Clause 8.1 (b), 8.9 (a), (c), (d) and (e);

(iii) Clause 9 (a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

(a) Where these Clauses use 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 5

Hierarchy

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

Clause 6

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.

Clause 7

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 the Appendix and signing Annex I.A.

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

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.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 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, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject 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 data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end 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. 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 that prohibit return or deletion of the personal data, the data importer warrants that it will continue 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).

8.6 Security of processing

(a) The data importer and, during 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 state of the art, the costs of implementation, 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, 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. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. 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 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 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, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, 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.

8.7 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 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (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, under the appropriate Module, or if:

(i) 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;

(ii) 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;

(iii) 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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

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

[2] 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.

(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.

(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 audits of the processing activities covered by these Clauses, 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.

(d) 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.

(e) The 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.

Clause 9

Use of sub-processors

(a) 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 two weeks prior to the engagement of the 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.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that 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.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure

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

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 the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless 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.

Clause 11

Redress

(a) 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. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) 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) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) 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 12

Liability

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

(b) 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 by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), 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 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 Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) 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.

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

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

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

Clause 13

Supervision

(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 Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(a) [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.

(a) [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) 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 is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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 enquiries, submit 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

(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[4];

(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 data importer agrees 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).

[4] 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 other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(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. 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 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

15.1 Notification

(a) 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:

(i) 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

(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.

(b) 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.

(c) 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.).

(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 on request.

(e) 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.

15.2 Review of legality and data minimisation

(a) 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).

(b) 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.

(c) 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 IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

(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 without prejudice to Clause 14(f).

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

(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;

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

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

In these cases, 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 relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. 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 that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) 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) 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 Regulation (EU) 2016/679.

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

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

A. **LIST OF PARTIES**

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

1. The data exporter(s) is/are the entities as identified in ANNEX IV that transfer(s) personal data to the data importer.

Signature and date: The undersigned has the power of attorney to sign for all data exporters listed in ANNEX IV.

Name: All data exporters listed in ANNEX IV

Address: See ANNEX IV

Contact person's name, position and contact details:

Signature and date:

Role controller/processor): Controller

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): Processor

2.…

In addition to these Clauses, the parties incorporate ANNEX VI below as an Annex to these Clauses.

To the extent the data exporter(s) is/are subject to the UK GDPR and the data importer is not located in a country recognized by the UK as providing an adequate level of data protection, which currently includes countries within the EU, the EEA, Gibraltar, Andorra, Argentina, Faeroe Island, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, Japan and Canada, the parties incorporate and agree on the UK Addendum to the EU Commission Standard Contractual Clauses issued by the Information Commissioner's Office under S119A(1) Data Protection Act 2018, VERSION B1.0, in force as of 21 March 2022 (or in the currently valid version in accordance with Section 18 UK Addendum). To the extent required, the Tables 1 to 3 of the UK Addendum shall be completed with the corresponding information in the Appendix of the Standard

Commented [A2]: Please provide us with the full name, legal form and address of the entity which is the data importer (receives the data in the third country outside of the EEA). Further, please provide the details on the contact person and information on the activities relevant to the data transfer.

Contractual Clauses. In addition, the Parties agree that no separate signature is required for the purposes of Section 2 UK Addendum (Table 1) and that neither Party may end the UK Addendum as set out in Section 19 UK Addendum (Table 4).

To the extent the data exporter(s) is/are subject to the Swiss Federal Data Protection Act (FDPA) and the data importer is not located in a country recognized by the Swiss Federal Data Protection and Information Commissioner (FDPIC) as providing an adequate level of data protection, which currently includes countries within the EU, the EEA, Gibraltar, Andorra, Argentina, Faeroe Island, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay and Canada, the parties agree to amend the Standard Contractual Clauses as follows, provided that none of these amendments will have the effect or be construed to amend the Standard Contractual Clauses in relation to the processing of personal data under the GDPR. In relation to personal data that is processed in and exported from Switzerland by the data exporter(s), references to a "member state" or to the "EU" in the Standard Contractual Clauses will be deemed to include Switzerland; references to Regulation (EU) 2016/679 will be deemed to be references to equivalent provisions of the FDPA; where the FDPA protects legal entities as data subjects, the Standard Contractual Clauses will apply to data relating to identified or identifiable legal entities; and the FDPIC will be the sole or, where both the FDPA and the GDPR apply to such transfer, one of the competent data protection authorities, under the Standard Contractual Clauses.

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

…

Categories of personal data transferred

…

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).

☐ One-off transfer ☐ Transfer on a continuous basis

Nature of the processing

…

Purpose(s) of the data transfer and further processing

…

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

…

C. **COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with Clause 13

Depending on the specific service(s) affected by the Clauses as well as the data exporter(s) involved the competent authority is the following:

eBay Marketplace Services:

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

Stahnsdorfer Damm 77

Commented [A3]: Please include the types of individuals affected by the data processing.
Example: Employees, users, customers, suppliers.

Commented [A4]: Please include the types of data categories affected by the data processing.
Example: names, email addresses, IP addresses, click data, banking details, working hours.

Commented [A5]: Please include the types of sensitive data categories affected by the data processing, if any.
Example: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Commented [A6]: Please select as applicable.

Commented [A7]: Please provide.
Example: The data importer assists the data exporter in complying with legal obligations.

Commented [A8]: Please describe the purposes for which you receive the data.
Example: The data is processed to provide marketing services for the data exporter.

Commented [A9]: Please provide information on the retention period.
Example: The data will be retained for six months. OR The data will be retained until the end of the contract with data exporter.

Commented [A10]: Please include, if applicable.

14532 Kleinmachnow

Tel: +49 33203/356-0

Fax: +49 33203/356-49

Email: Poststelle@LDA.Brandenburg.de

eBay Payment Services:

Commission Nationale pour la Protection des Données

15, Boulevard du Jazz

L-4370 Belvaux

Tel: +352 2610 60 1

Fax: +352 2610 60 6099

Email: info@cnpd.lu

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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.

Commented [A11]: Please select as applicable and provide description of the measures.

The data importer uses, as far as possible, strong encryption for the transport and storage of personal data (transport encryption and data-at-rest encryption). Strong encryption requires that

(a) transport encryption is used for which it is ensured that the encryption protocols employed are state-of-the-art and provide effective protection against active and passive attacks with resources known to be available to the public authorities of the third country;

(b) the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and to be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them;

(c) the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved;

(d) the encryption algorithm is flawlessly implemented by properly maintained software.

☐ Further measures of pseudonymisation and encryption of personal data

Description: …

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

Description: …

☐ 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

Description: …

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

Description: …

☐ Measures for user identification and authorization

Description: …

☐ Measures for the protection of data during transmission

Description: …

☐ Measures for the protection of data during storage

Description: …

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

Description: …

☐ Measures for ensuring events logging

Description: …

☐ Measures for ensuring system configuration, including default configuration

Description: …

☐ Measures for internal IT and IT security governance and management

Description: …

☐ Measures for certification/assurance of processes and products

Description: …

☐ Measures for ensuring data minimization

Description: …

☐ Measures for ensuring data quality

Description: …

☐ Measures for ensuring limited data retention

Description: …

☐ Measures for ensuring accountability

Description: …

☐ Measures for allowing data portability and ensuring erasure

Description: …

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (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

☐ For transfers to (sub-) processors: The (sub-) processor has taken sufficient technical and organisational measures to be able to provide assistance to the controller.

Description: …

☐ For transfers from a processor to a sub-processor: The sub-processor has taken sufficient technical and organisational measures to be able to provide assistance to the data exporter.

Description: …

☐ Not applicable

Further, the Parties agree on the Supplementary Measures as listed in ANNEX V.

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed, 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. . . . .

Commented [A12]: Please include details on sub-processors.

ANNEX IV

DATA EXPORTER

The following entities may act as data exporters under these Clauses, as applicable:

Role of the data exporter/s: Controller

Activities relevant to the data transferred under these Clauses: See Annex I, Section B.

	Name	Address	Contact person's name, position and contact details
1.	eBay GmbH	Albert-Einstein-Ring 2-6, 14532 Kleinmachnow, Germany	Miriam Hui Legal Director See company address
2.	eBay (UK) Limited	1 More London Place, London, SE1 2AF, United Kingdom	Kumaran Adithyan COO UK
3.	eBay Marketplaces GmbH	Helvetiastrasse 15/17, 3005 Bern, Switzerland	Jana Skottova Senior Director, Accounting
4.	eBay S.à.r.l.,	22-24 Boulevard Royal, L-2449 Luxembourg	Olivier Hoen Authorised Manager
5.	eBay Commerce UK Ltd	1 More London Place, London SE1 2AF, United Kingdom	Alec Latimer Director
6.	eBay Customer Support GmbH	Albert-Einstein-Ring 2-6, 14532, Kleinmachnow, Germany	Jens Voigt Director GPM iRegiona and Global Functions
7.	eBay Group Services GmbH	Albert-Einstein-Ring 2-6, 14532, Kleinmachnow, Germany	Alexander Sirzisko Director Finance

8.	eBay International Management B.V.	Wibaustraat 224, 1097 DN, Amsterdam, Netherlands	Carel Van Spanje Group controller Ken Ebanks Vice President, Director
9.	EU Liaison Office BVBA	Kunstlaan 44, 1040 Brussel, Belgium	Stefan Krawczyk Director
10.	eBay Services S.a.r.l.	22-24 Boulevard Royal, 5th Flr., 2449, Luxembourg, Luxembourg	Olivier Hoen Authorised Manager Michael Verlaque Director
11.	eBay Europe Services Limited	The Atrium, Old Navan Road, Blanchardstown, Dublin 15, Ireland	Hazel Mitchell Senior Director
12.	eBay GmbH, succursale France	21, rue de la Banque, 75002, Paris, France	Nathalie Vuaillat Directeur General eBay France SAS
13.	eBay France SAS	21, rue de la Banque, 75002, Paris, France	Nathalie Vuaillat Directeur General eBay France SAS
14.	eBay (UK) Limited, sede secondaria, Milano	Via Roberto Lepetit 8/10, 20124, Milano, Italy	Alice Acciarri General Manager, Italy
15.	eBay Spain International, S.L.	Paseo de la Castellana, 216, 9th floor, 28046 Madrid, Spain	Pedro Lopez Administrador Único
16.	eBay Czech Republic s.r.o..	Nile House, Karolinska 654/2, Prague 8, Karlin, Prague 186 00, Czech Republic	Sylke Maringer Director CM Business Operations and Operational Excellence

ANNEX V

ADDITIONAL SAFEGUARDS TO THE STANDARD CONTRACTUAL CLAUSES ("SUPPLEMENTARY MEASURES")

(A) Following the Parties' joint effort to assess the risks for data subjects affected by the respective data processing activities of the Parties, the Parties decided to supplement the Clauses as set out in the following.

(B) Nothing in these Supplementary Measures shall limit or exclude any rights of data subjects granted in the Clauses or applicable data protection laws, in particular the General Data Protection Regulation (GDPR) or any obligations of either Party arising from or in connection with the Clauses.

1. General requirements

The Parties undertake to adapt or replace these Supplementary Measures as soon as the European Commission makes available any mechanism that provides adequate safeguards for the transfer of personal data to the data importer. The same applies to adjustments following recommendations of the European Commission and/or the competent data protection authorities.

2. Processing restrictions

Data importer will not disclose personal data except (1) as data exporter directs or (2) where the transfer is in accordance with the provisions of the Clauses and these Supplementary Measures.

3. Data access for public authorities

Notwithstanding Clause 15 of the Clauses, data importer warrants the following:

3.1 Data importer agrees to adopt

(a) adequate internal policies with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for cases of covert or official requests from public authorities to access the data;

(b) strict and granular data access and confidentiality policies and best practices, based on a strict need-to-know principle.

Data importer will regularly review these internal policies to assess their suitability and identify and implement additional or alternative solutions when necessary.

3.2 If data importer is contacted with a legally binding request from a public authority, including judicial authorities, or becomes aware of any direct access by a public authority to the personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination, data importer will attempt to redirect the public authority to request that personal data directly from data exporter instead.

3.3 Data importer will only provide personal data if, and to the extent that, it is necessary and proportionate to comply with a legally binding request. Data importer will not provide any public authority:

(a) blanket, or unfettered access to personal data;

(b) encryption keys used to secure personal data or the ability to break such encryption; or

(c) access to personal data if data importer is aware that the personal data is to be used for purposes other than those stated in the legally binding request.

3.4 In support of the above, data importer may provide data exporter's basic contact information to the public authority. The data importer will notify data exporter in this case, unless data importer is legally restricted to do so.

3.5 The data importer agrees to document the steps taken pursuant to Sections 3.1-3.4 for the duration of the contract and make it available to the competent supervisory authority upon request.

4. Encryption

The data importer warrants that that (1) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data, (2) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and (3) that national law or government policy does not require the importer to create or maintain back doors or to facilitate access to personal data or systems or for the importer to be in possession or to hand over the encryption key.

ANNEX VI

BASIS FOR TRANSFER IMPACT ASSESSMENT PURSUANT TO CLAUSE 14 OF THE CLAUSES

Pursuant to Clause 14(b), the Parties undertake to use the questionnaire provided by the data exporter to collect the relevant information as basis for conducting a Transfer Impact Assessment. The Parties' warranty in accordance with Clause 14(a) is based on the information provided by the data importer through the aforementioned questionnaire, as incorporated in this ANNEX VI.

Commented [A13]: Please include answers to questionnaire.