Google Ads Data Processing Terms: EU Standard Contractual Clauses (Module 2: 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) 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.

(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 44(2) 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 – Clause 8.1(b), 8.1(a), (c), (d) and (e);
(iii) Clause 9 – Clause 9(a), (b), (d) and (e);
(iv) Clause 12 – Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(a);
(viii) Clause 18 – 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 - Not used

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 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(a) 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.

(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 (7) (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:
8.9 Documentation and compliance

(a) GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s).

(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. The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. 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 fulfill 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 9
Use of sub-processors

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 the data subject’s habitual residence or place of work, or of 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(5) 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 either substantive or procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability
Clause 13  
Supervision

(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. 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 12(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 (c);

(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).

(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 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
Choice of forum and jurisdiction

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 Ireland.

(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.
ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Customer
Address: As specified in the Agreement.
Contact person’s name, position and contact details: Contact details for the data exporter are specified in the Agreement. Details about the data exporter’s data protection officer (or, where the data exporter has not appointed a data protection officer, another appropriate point of contact) are available to the data importer in the form of the Notification Email Address.
Activities relevant to the data transferred under these Clauses: The data importer provides the Processor Services to the data exporter in accordance with the Agreement.
Signature and date: The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of these Clauses by both parties as follows:
In respect of the transfer of Customer Personal Data pursuant to the EU GDPR and/or the Swiss FDPA in accordance with Section 10.2 (Restricted European Transfers) of the Data Processing Terms:
(a) on 22 September 2022, where the effective date of the Agreement is on or before 21 September 2022; or
(b) otherwise, on the effective date of the Agreement.

In respect of the transfer of Customer Personal Data pursuant to the UK GDPR in accordance with Section 10.2 (Restricted European Transfers) of the Data Processing Terms:
(a) on 22 September 2022, where the effective date of the Agreement is on or before 21 September 2022; or
(b) otherwise, on the effective date of the Agreement.

Role (controller/processor): controller

Data importer(s):

Name: Google
Address: As specified in the Agreement.
Contact person’s name, position and contact details: Contact details for the data importer are specified in the Agreement. The data importer’s data protection team can be contacted as described in the Data Processing Terms.
Activities relevant to the data transferred under these Clauses: The data importer provides the Processor Services to the data exporter in accordance with the Agreement.
Signature and date: The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of these Clauses by both parties as follows:
In respect of the transfer of Customer Personal Data pursuant to the EU GDPR and/or the Swiss FDPA in accordance with Section 10.2 (Restricted European Transfers) of the Data Processing Terms:
(a) on 27 October 2021, where the effective date of the Agreement is before 27 September 2021; or
(b) otherwise, on the effective date of the Agreement.

In respect of the transfer of Customer Personal Data pursuant to the UK GDPR in accordance with Section 10.2 (Restricted European Transfers) of the Data Processing Terms:
(a) on 27 October 2021, where the effective date of the Agreement is on or before 21 September 2022; or
(b) otherwise, on the effective date of the Agreement.

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The personal data transferred concern the following categories of data subjects:

- data subjects about whom Google collects personal data in its provision of the Processor Services; and/or
- data subjects about whom personal data is transferred to Google in connection with the Processor Services by, at the direction of, or on behalf of Customer.

Depending on the nature of the Processor Services, these data subjects may include individuals: (a) to whom online advertising has been, or will be, directed; (b) who have visited specific websites or applications in respect of which Google provides the Processor Services; and/or (c) who are customers or users of Customer’s products or services.

Categories of personal data transferred

Customer Personal Data may include the types of personal data described at business.safety.google/adsservices.

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.

Not applicable.

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

Customer Personal Data may be transferred on a continuous basis until it is deleted in accordance with the terms of the Data Processing Terms.

Nature of the processing

The personal data transferred will be subject to the following basic processing activities: as applicable to the Processor Services and the instructions of the data exporter, collecting, recording, organising, structuring, storing, altering, retrieving, using, disclosing, combining, erasing and destroying personal data for the purpose of providing the Processor Services and any related technical support to the data exporter in accordance with the Data Processing Terms.

Purpose(s) of the data transfer and further processing

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 or category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.
The data importer will process Customer Personal Data to provide the Processor Services and related technical support in accordance with the Agreement.

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

For the duration of the Agreement until deletion in accordance with the provisions of the Data Processing Terms.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing

As above.

C. COMPETENT SUPERVISORY AUTHORITY

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

The Irish Supervisory Authority - The Data Protection Commission, unless the data exporter notifies the data importer of an alternative competent supervisory authority from time to time in accordance with Section 12.2 of the Data Processing Terms.

ANNEX II

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

The data importer abides by the security standards set out in Appendix 2 to the Data Processing Terms.

The technical and organisational measures taken by the data importer to 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 are set out in Sections 8 (Impact Assessments and Consultations) and 9 (Data Subject Rights) of the Data Processing Terms.

ANNEX III

LIST OF SUB-PROCESSORS

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

business.safety.google/adssubprocessors

ANNEX IV

SUPPLEMENTARY TERMS FOR SWISS FDPA TRANSFERS ONLY

The following terms supplement the Clauses only if and to the extent the Clauses apply with respect to data transfers subject to the Federal Data Protection Act of 19 June 1992 (Switzerland):

1. The term ‘Member State’ will be interpreted in such a way as to allow data subjects in Switzerland to exercise their rights under the Clauses in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Clauses.

ANNEX V

SUPPLEMENTARY TERMS FOR UK GDPR TRANSFERS ONLY

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

<table>
<thead>
<tr>
<th>Start date</th>
<th>The Parties</th>
<th>Importer (who receives the Restricted Transfer)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start date</td>
<td>Exporter (who sends the Restricted Transfer)</td>
<td>Importer (who receives the Restricted Transfer)</td>
</tr>
<tr>
<td>(a) 21 September 2022, where the effective date of the Agreement is before 21 September 2022; or (b) otherwise, on the effective date of the Agreement.</td>
<td>Full legal name: Customer Trading name (if different): As specified in the Agreement. Main address (if a company registered address): As specified in the Agreement. Official registration number (if any) (company number or similar identifier): As specified in the Agreement.</td>
<td>Full legal name: Google Trading name (if different): As specified in the Agreement. Main address (if a company registered address): As specified in the Agreement. Official registration number (if any) (company number or similar identifier): As specified in the Agreement.</td>
</tr>
<tr>
<td>Parties’ details</td>
<td>Contact details for the data exporter are specified in the Agreement. Details about the data</td>
<td>Contact details for the data importer are specified</td>
</tr>
</tbody>
</table>
Addendum EU SCCs

The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:

Table: Appendix Information

<table>
<thead>
<tr>
<th>Key Contact</th>
<th>The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of this Addendum.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of this Addendum.</td>
</tr>
</tbody>
</table>

Date: 4 June 2021
Reference (if any): Module 2: Controller-to-Processor
Other identifier (if any): N/A

Part 2: Mandatory Clauses

Mandatory Clauses

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Table 2: Selected SCCs, Modules and Selected Clauses

<table>
<thead>
<tr>
<th>Addendum EU SCCs</th>
<th>The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Date: 4 June 2021</td>
</tr>
<tr>
<td>Reference (if any)</td>
<td>Reference (if any): Module 2: Controller-to-Processor</td>
</tr>
<tr>
<td>Other identifier (if any)</td>
<td>Other identifier (if any): N/A</td>
</tr>
</tbody>
</table>

Table 3: Appendix Information

“Appendix Information” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex IA: List of Parties: Annex I(A)
Annex IB: Description of Transfer: Annex I(B)
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Annex II
Annex III: List of Sub processors (Modules 2 and 3 only): Annex III

Table 4: Ending this Addendum when the Approved Addendum Changes

<table>
<thead>
<tr>
<th>Ending this Addendum when the Approved Addendum changes</th>
<th>Which Parties may end this Addendum as set out in Section 19:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✔ Importer</td>
</tr>
<tr>
<td></td>
<td>✔ Exporter</td>
</tr>
<tr>
<td></td>
<td>☐ neither Party</td>
</tr>
</tbody>
</table>

Part 2: Mandatory Clauses

Mandatory Clauses

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

---

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 25(6) of Regulation (EU) 2018/1725 of the European Parliament and 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 2271/2001/EC (OJ L 39, 21.1.2001, 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 25(5) of Regulation (EU) 2016/679 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2020/59.

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.

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

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, shown 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.