# Google Ads Controller-Controller Data Protection Terms: EU Standard Contractual Clauses (Module 1: Controller-to-Controller)

## 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.

(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 – Clause 8.5 (e) and Clause 8.9(b);

(iii) Clause 9 – Not applicable

(iv) Clause 12 – Clause 12(a) and (d);

(v) Clause 13;

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

(vii) Clause 16(e);

(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 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. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

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

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

**8.2 Transparency**

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

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

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

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

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.3 Accuracy and data minimisation**

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

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

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

**8.4 Storage limitation**

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

**8.5 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the 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 subject. 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.

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

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

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

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

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together

with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

**8.6 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 or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

**8.7 Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union ([3]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

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

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

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

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

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

**8.8 Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

**8.9 Documentation and compliance**

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

## Clause 9 - *Not applicable*

## Clause 10

## Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. ([4]) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

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

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

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

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

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

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

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

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

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

## 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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

(e) The data importer may not invoke the conduct of a processor or 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.

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 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(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:

(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 Ireland.

## 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.

# 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 be 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):**

As applicable in accordance with Section 6 (Controller SCCs) of the Controller Terms, either:

1. Name: Google Ireland Limited

   Address: Gordon House Barrow Street Dublin 4, Ireland

   Contact person's name, position and contact details: Google's data protection team can be contacted at - https://support.google.com/policies/troubleshooter/9009584

   OR

2. Name: Google LLC

   Address: 1600 Amphitheatre Parkway, Mountain View, California 94043, USA

   Contact person's name, position and contact details: Google's data protection team can be contacted at - https://support.google.com/policies/troubleshooter/9009584

   OR

3. Name: Customer

   Address: As set out in the Agreement

   Contact person's name, position and contact details: Contact details for the Customer are specified in, or supplied to Google in connection with, the Agreement.

Activities relevant to the data transferred under these Clauses: Google provides the Controller Services and Customer uses the Controller Services; Google processes personal data as described in Google's Privacy Policy at https://policies.google.com/privacy.

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 European Controller Personal Data in accordance with Section 6.1 (Transfers of European Controller Personal Data to Customer) of the Controller Terms:

(a) on 27 October 2021, where the effective date of the Agreement is on or before 27 September 2021; or

(b) otherwise, on the effective date of the Agreement.

In respect of the transfer of UK Controller Personal Data in accordance with Sections 6.2 (Transfers of UK Controller Personal Data to Customer) and 6.4 (Transfers of UK Controller Personal Data to Google) of the Controller Terms:

(a) on 21 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):**

As applicable in accordance with Section 6 (Controller SCCs) of the Controller Terms, either:

1. Name: Customer

   Address: As set out in the Agreement

   Contact person's name, position and contact details: Contact details for the Customer are specified in, or supplied to Google in connection with, the Agreement.

   OR

2. Name: Google LLC

   Address: 1600 Amphitheatre Parkway, Mountain View, California 94043, USA

   Contact person's name, position and contact details: Google's data protection team can be contacted at - https://support.google.com/policies/troubleshooter/9009584

Activities relevant to the data transferred under these Clauses: Google provides the Controller Services and Customer uses the Controller Services; Google processes personal data as described in Google's Privacy Policy at https://policies.google.com/privacy.

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 European Controller Personal Data in accordance with Section 6.1 (Transfers of European Controller Personal Data to Customer) of the Controller Terms:

(a) on 27 October 2021, where the effective date of the Agreement is on or before 27 September 2021; or

(b) otherwise, on the effective date of the Agreement.

In respect of the transfer of UK Controller Personal Data in accordance with Sections 6.2 (Transfers of UK Controller Personal Data to Customer) and 6.4 (Transfers of UK Controller Personal Data to Google) of the Controller Terms:

(a) on 21 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

**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 (as defined in the Controller Terms) collects personal data in its provision of the Controller Services (as defined in the Controller Terms); and/or
- data subjects about whom personal data is transferred to or from Google in connection with the Controller Services by, at the direction of, or on behalf of the data exporter.

Depending on the nature of the Controller 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 Controller Services; and/or (c) who are customers or users of the products or services of Customer (as defined in the Controller Terms).

*Categories of personal data transferred*

The personal data transferred concern the following categories of data: the categories of personal data described at https://policies.google.com/technologies/ads and https://policies.google.com/technologies/partner-sites.

*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).*

Personal data may be transferred from time to time in accordance with the Agreement.

*Nature of the processing*

Google will process (including, collecting, recording, organising, structuring, storing, altering, retrieving, using, disclosing, combining, erasing and destroying) personal data for the purpose of providing the Controller Services and any related technical support to Customer in accordance with the Controller Terms.

*Purpose(s) of the data transfer and further processing*

The transfer is made for the following purposes:

- to facilitate the provision of the Controller Services by Google and/or the use of the Controller Services by Customer; and
- in the case of Google, for the purposes described in Google's Privacy Policy at https://policies.google.com/privacy.

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

(a) Where Customer is data importer: The period for which the personal data will be retained will be determined by the importing Customer in accordance with its data privacy and data retention policies.

(b) Where Google is data importer: The period for which the personal data will be retained will be determined in accordance with the data retention practices described at https://policies.google.com/technologies/ads.

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

Not Applicable

**C. COMPETENT SUPERVISORY AUTHORITY**

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

The Irish Supervisory Authority - The Data Protection Commission

# 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.*

PART A: Customer as data importer:

*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.*

The data importer has implemented measures at least equivalent to the technical and organisational measures described below, in addition to any other measures specified in, or supplied to Google in connection with, the Agreement.

**1. Information Security Policy**

Customer has a documented information security policy which its personnel are aware of and comply with.

**2. Organisation of Information Security**

Customer has organised its operations in such a manner that it is clear as to which individual(s) in the Customer's organisation have responsibility for information security. Customer defines, establishes and documents basic security processes to include, but not be limited to: information risk assessments; incident response; patch management; vulnerability monitoring; security awareness education and training for its personnel (as appropriate to its operations).

Customer has controls to reduce the risk associated when outsourcing services, including but not limited to: specifying security and confidentiality requirements; restricting

subcontractor access to only those areas of the system(s) that are necessary to perform the outsourced service(s), generating event logs on systems and networks that have been accessed; and analysing the event logs.

**3. Physical and Environmental Security**

Customer executes measures necessary to limit the risk of operational disturbance, theft, natural disasters and unauthorised access to data.

Customer ensures that only authorised users have physical access to the network, critical systems and applications, server rooms, communication rooms and work environments. Customer provides secure protection for its physical facilities (e.g. through card readers, key cards or a tended reception area).

**4. Communications and Operations Management**

To ensure the confidentiality, integrity and availability of data, Customer applies proper security controls.

4.1. Customer has controls in place to detect and prevent malicious code from being executed on any system. These controls are regularly updated, and the most recent versions of antivirus signatures are distributed as soon as reasonably practicable to ensure detection and prevention of malicious attacks.

4.2. Customer ensures that there are reasonable controls in place when backing up data, such as event logs and reviews of those; the backup media is encrypted, where possible, using strong encryption; backup restoration testing is performed regularly; and procedures are in place to ensure backup media will operate in the event of an emergency.

4.3. Customer ensures that all external entry points to network segments containing data have access controls in place.

4.4. Customer ensures that the databases and repositories containing data are protected from unauthorised access by using appropriate authorisation controls. The databases and connections to the databases are encrypted.

4.5. Customer ensures that controls for the operating system and applications are in place to prevent unauthorised access to system documentation.

4.6. Customer has a secure electronic messaging system to prevent unauthorised access. All incoming and outgoing emails are scanned.

4.7. Customer has controls to prevent unauthorised access to external or internet exposed applications and the information in those applications.

**5. Access control**

Customer has in place formal processes and procedures to support the secure creation, amendment and deletion of user accounts.

5.1. Access is only granted to individuals needing access in order to perform a certain role, function or responsibility.

5.2. Customer ensures that access control mechanisms based on passwords are enforced by automated means.

5.3. Customer has controls in place that enable reviews of user access rights with particular focus on 'privileged users' (e.g. sys administrator).

5.4. Customer ensures that remote access to systems and applications containing data are governed by appropriate authentication (e.g. two-factor authentication), and that such access is encrypted (e.g. VPN).

5.5. Customer ensures that only authorised users can connect to wired or wireless network segments, if such segments exist.

5.6. Customer applies a level of security for its own wireless network that is equivalent to the level of protection achieved using VPN. Traffic supports strong encryption and strong authentication.

5.7. Customer ensures that access to operating system used to store or process data use secure logon mechanisms.

5.8. Customer has a policy in place to prevent the spread of information from mobile computing such as portable computers and smartphones.

**6. External operating of applications and maintenance of software and services**

6.1. Customer has security controls of software, services and systems that process or make data accessible.

6.2. Customer has processes and systems for patch management (where appropriate).

6.3. Customer ensures that web-based products are reasonably protected against attack.

**7. Information Security Incident Management**

In order to maintain business operations Customer has a formalised security incident handling process in place.

**8. Business Continuity Management**

Customer ensures that Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) are documented and tested on a regular basis to ensure operational continuity (to the extent necessary for its operations).

*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*

Not applicable.

PART B: Google as data importer

*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.*

As from the Terms Effective Date, Google will implement and maintain technical and organisational measures to protect Controller Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access as described in this Part B of Annex II ("**Security Measures**"). Google may update or modify such Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Controller Services.

**1. Data Centre & Network Security**

**(a) Data Centres.**

**Infrastructure**. Google maintains geographically distributed data centres. Google stores all production data in physically secure data centres.

**Redundancy**. Infrastructure systems have been designed to eliminate single points of failure and minimise the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Controller Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data centre equipment is scheduled through a standard process according to documented procedures.

**Power**. The data centre electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data centre. Backup power is provided by various mechanisms such as uninterruptible power supply (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data centre, at full capacity, for up to 10 minutes until the backup generator systems take over. The backup generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data centre at full capacity typically for a period of days.

**Server Operating Systems**. Google servers use hardened operating systems which are customised for the unique server needs of the business. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used to provide the Controller Services and enhance the security products in production environments.

**Business Continuity**. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

**Encryption Technologies**. Google's security policies mandate encryption at rest for all user data, including personal data. Data is often encrypted at multiple levels in Google's production storage stack in data centres, including at the hardware level, without requiring any action by customers. Using multiple layers of encryption adds redundant data protection and allows Google to select the optimal approach based on application requirements. All personal data is encrypted at the storage level, generally using AES256. Google uses common cryptographic libraries which incorporate Google's FIPS 140-2 validated module, to implement encryption consistently across the Controller Services.

**(b) Networks & Transmission.**

**Data Transmission**. Data centres are typically connected via high-speed private links to provide secure and fast data transfer between data centres. Further, Google encrypts data transmitted between data centres. This is designed to prevent data from being read, copied, altered or removed without authorisation during electronic transport. Google transfers data via Internet standard protocols.

**External Attack Surface**. Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

**Intrusion Detection**. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves:

1. Tightly controlling the size and make-up of Google's attack surface through preventative measures;
2. Employing intelligent detection controls at data entry points; and
3. Employing technologies that automatically remedy certain dangerous situations.

**Incident Response**. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.

**Encryption Technologies**. Google makes HTTPS encryption (also referred to as TLS connection) available. Google servers support ephemeral elliptic curve Diffie Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimise the impact of a compromised key, or a cryptographic breakthrough.

**2. Access and Site Controls**

**(a) Site Controls.**

**On-site Data Centre Security Operation**. Google's data centres maintain an on-site security operation responsible for all physical data centre security functions 24 hours a day, 7 days a week. The on-site security operations personnel monitor Closed Circuit TV ("CCTV") cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data centre regularly.

**Data Centre Access Procedures**. Google maintains formal access procedures for allowing physical access to the data centres. The data centres are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data centre are required to identify themselves as well as show proof of identity to on-site security operations. Only authorised employees, contractors and visitors are allowed entry to the data centres. Only authorised employees and contractors are permitted to request electronic card key access to these facilities. Data centre electronic card key access requests must be made in advance and in writing, and require the approval of authorised data centre personnel. All other entrants requiring temporary data centre access must: (i) obtain approval in advance from authorised data centre personnel for the specific data centre and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data centre access record identifying the individual as approved.

**On-site Data Centre Security Devices**. Google's data centres employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorised activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorised access throughout the business operations and data centres is restricted based on zones and the individual's job responsibilities. The fire doors at the data centres are alarmed. CCTV cameras are in operation both inside and outside the data centres. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data centre building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centres connect the CCTV equipment. Cameras record on-site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for at least 7 days based on activity.

**(b) Access Control.**

**Infrastructure Security Personnel**. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Controller Services, and responding to security incidents.

**Access Control and Privilege Management**. Customer's administrators and users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Controller Services.

**Internal Data Access Processes and Policies – Access Policy**. Google's internal data access processes and policies are designed to prevent unauthorised persons and/or systems from gaining access to systems used to process personal data. Google aims to design its systems to: (i) only allow authorised persons to access data they are authorised to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralised access management system to control personnel access to production servers, and only provides access to a limited number of authorised personnel. LDAP, Kerberos and a proprietary system utilising digital certificates are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimise the potential for unauthorised account use. The granting or modification of access rights is based on: the authorised personnel's job responsibilities; job duty requirements necessary to perform authorised tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g. login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength.

**3. Data**

**(a) Data Storage, Isolation & Authentication.**

Google stores data in a multi-tenant environment on Google-owned servers. Data, the Controller Services database and file system architecture are replicated between multiple geographically dispersed data centres. Google logically isolates each customer's data. A central authentication system is used across all Controller Services to increase uniform security of data.

**(b) Decommissioned Disks and Disk Destruction Guidelines.**

Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Data Destruction Guidelines") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Data Destruction Guidelines.

**(c) Pseudonymous Data.**

Online advertising data are commonly associated with online identifiers which on their own are considered 'pseudonymous' (i.e. they cannot be attributed to a specific individual without the use of additional information). Google has a robust set of policies and technical and organisational controls in place to ensure the separation between pseudonymous data and personally identifiable user information (i.e. information that could be used on its own to directly identify, contact, or precisely locate an individual), such as a user's Google account data. Google policies only allow for information flows between pseudonymous and personally identifiable data in strictly limited circumstances.

**(d) Launch reviews.**

Google conducts launch reviews for new products and features prior to launch. This includes a privacy review conducted by specially trained privacy engineers. In privacy reviews, privacy engineers ensure that all applicable Google policies and guidelines are followed, including but not limited to policies relating to pseudonymisation and data retention and deletion.

4. **Personnel Security**

Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Controller Personal Data are required to complete additional requirements appropriate to their role. Google's personnel will not process Controller Personal Data without authorisation.

5. **(Sub)processors**

In this paragraph, "**(Sub)processors**" means a third party appointed by Google to have logical access to and process Controller Personal Data in order to provide parts of the Controller Services and any related technical support.

Before onboarding (Sub)processors, Google conducts an audit of the security and privacy practices of (Sub)processors to ensure (Sub)processors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the (Sub)processor, the (Sub)processor is required to enter into appropriate security, confidentiality and privacy contract terms. Google will ensure via a written contract that (i) the (Sub)processor only accesses and uses Controller Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including the Controller Terms); and (ii) if the processing of Controller Personal Data is subject to the European Data Protection Legislation, the data protection obligations in Article 28(3) of the GDPR are imposed on the (Sub)processor.

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

Not Applicable

# ANNEX III

**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 IV

**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

| | | |
|---|---|---|
| **Start date** | (a) 21 September 2022, where the effective date of the Agreement is before 21 September 2022; or<br>(b) otherwise, on the effective date of the Agreement. | |
| **The Parties** | **Exporter (who sends the Restricted Transfer)** | **Importer (who receives the Restricted Transfer)** |
| **Parties' details** | As applicable in accordance with Section 6 (Controller SCCs) of the Controller Terms:<br>Full legal name: Customer<br>Trading name (if different): As specified in the Agreement.<br>Main address (if a company registered address): As specified in the Agreement.<br>Official registration number (if any) (company number or similar identifier): As specified in the Agreement.<br>OR<br>Full legal name: Google LLC<br>Trading name (if different): N/A.<br>Main address (if a company registered address): 1600 Amphitheatre Parkway, Mountain View, California 94043, USA<br>Official registration number (if any) (company number or similar identifier): 3582691 | As applicable in accordance with Section 6 (Controller SCCs) of the Controller Terms:<br>Full legal name: Customer<br>Trading name (if different): As specified in the Agreement.<br>Main address (if a company registered address): As specified in the Agreement.<br>Official registration number (if any) (company number or similar identifier): As specified in the Agreement.<br>OR<br>Full legal name: Google LLC<br>Trading name (if different): N/A.<br>Main address (if a company registered address): 1600 Amphitheatre Parkway, Mountain View, California 94043, USA<br>Official registration number (if any) (company number or similar identifier): 3582691 |
| **Key Contact** | Contact details for the Customer are specified in the Agreement.<br>Google's data protection team can be contacted as described in the Controller Terms. | Contact details for the Customer are specified in the Agreement.<br>Google's data protection team can be contacted as described in the Controller Terms. |
| **Signature (if required** | The parties agree that execution of the Agreement by the data | The parties agree that execution of the Agreement by the data |

| | | |
|---|---|---|
| **for the purposes of Section 2)** | importer and the data exporter shall constitute execution of this Addendum. | importer and the data exporter shall constitute execution of this Addendum. |

## Table 2: Selected SCCs, Modules and Selected Clauses

| | |
|---|---|
| **Addendum EU SCCs** | The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:<br>Date: 4 June 2021<br>Reference (if any): Module 1: Controller-to-Controller<br>Other identifier (if any): N/A |

## 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 1A: List of Parties: Annex I(A)

Annex 1B: 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): N/A

## Table 4: Ending this Addendum when the Approved Addendum Changes

| | |
|---|---|
| **Ending this Addendum when the Approved Addendum changes** | Which Parties may end this Addendum as set out in Section 19:<br>✔ Importer<br>✔ Exporter<br>☐ neither Party |

# 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 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.

([2]) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

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

([4]) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.