Data Processing Addendum

This Optimizely Data Processing Addendum (**"DPA"**) is entered by and between the Optimizely entity (**"Optimizely"** or **"Data Processor"**) and Customer identified below (**"Customer"** or **"Data Controller"**). Provision of the Optimizely Service is subject to Optimizely's online terms of service (https://www.optimizely.com/terms/) or a signed agreement, if any, between Customer and Optimizely for provision of the Optimizely Service (as applicable, the **"Agreement"**). Capitalized terms not expressly defined here have the same meanings as in the Governing Agreement.

Accepted and agreed to as of the DPA Effective Date by the authorized representative of each party:

DPA Effective Date:			
Optimizely Entity:	Optimizely, Inc.	**Customer:**	
Address:		**Address:**	
Email:	privacy@optimizely.com	**Email:**	
Attention:	Legal Department	**Attention:**	
Signature:		**Signature:**	
Print Name:		**Print Name:**	
Title:		**Title:**	
Date:		**Date:**	

1. **OVERVIEW OF PROCESSING.** Customer and Optimizely have entered into a Governing Agreement for provision of the Optimizely Service to Customer. This DPA, which is incorporated as an attachment to that agreement, describes the parties' respective data protection obligations for the Personal Data processed on the Optimizely Service. With respect to this Personal Data, the parties agree that: **(i)** Customer is the controller under the GDPR and will comply with its controller obligations under applicable Data Protection Laws; and **(ii)** Optimizely is the processor under the GDPR and will comply with its data processor obligations under applicable Data Protection Laws.

2. **INSTRUCTIONS FOR PROCESSING.** Optimizely is authorized to process Customer's Personal Data only in accordance with the Instructions, as defined below. Customer will ensure that it has all necessary rights and permissions to permit Personal Data to be processed in accordance with these Instructions and that it will provide Personal Data to Optimizely only to the extent permitted by, and in compliance with, the Governing Agreement. Any additional Instructions must be agreed to in writing by Customer and Optimizely.

3. **PERSONNEL.** Optimizely will ensure that its and its Affiliate's employees and contractors who have access to Personal Data are subject to a written or legal obligation to maintain the confidentiality of that data and are adequately instructed in the good handling of Personal Data. Optimizely will implement measures to restrict employee access to Personal Data as set out in the Security Standards.

4. **SECURITY MEASURES.** Optimizely will implement appropriate technical and organisational security measures designed to protect Personal Data processed by the Optimizely Service against unauthorised or unlawful processing, accidental or unlawful destruction, accidental loss or alteration, and unauthorised disclosure or access. Optimizely's current measures are specified here[1] (the "**Security Standards**"). Optimizely may modify its technical and organisational security measures from time to time to reflect process improvements or changing practices, provided that such modifications do not result in an overall degradation of the security measures specified in the Security Standards. Without limiting Section 5 (Subprocessors) below, Optimizely has no responsibility for Customer's systems or Third-Party Products, including for their security, availability, integrity or data processing activities. Customer agrees that it is solely responsible for its own use of the Optimizely Service, including securing its account authentication credentials and choosing appropriate privacy and security settings.

[1] https://www.optimizely.com/security/

5. SUBPROCESSORS. Optimizely and its Affiliates may engage subprocessors to help provide the Optimizely Service and related services. Optimizely will ensure that the Affiliates and subprocessors it engages to process Personal Data agree to contractual requirements for confidentiality, data protection, and data security substantially equivalent to those set out in this DPA. Optimizely's list of subprocessors for the Optimizely Services is currently available here[2]. Optimizely will notify Customer by email of any changes concerning the addition or replacement of subprocessors on its subprocessor list, including changes to the location of processing. Customer may reasonably object to any newly-appointed subprocessor provided it sends Optimizely a written explanation of its objection within thirty (30) days of the change. In such cases, Optimizely will use commercially reasonable efforts to address the objection (such as by finding a suitable work around) or it will allow Customer to terminate its Order Form for the affected Optimizely Service if the change would cause Customer to be in breach of its obligations under applicable Data Protection Laws. Customer acknowledges that it may use the Optimizely Service with Third-Party Products and that these products are not subprocessors or subcontractors of Optimizely.

6. TRANSFERS.

6.1 In General. Subject to this Section, Customer authorizes Optimizely to transfer Personal Data to countries where Optimizely's Affiliates and subprocessors operate their systems (as specified on Optimizely's subprocessor list) and to other countries in response to Customer's written instructions or user-initiated actions on the Optimizely Service. Customer will comply with its responsibilities and obligations under Data Protection Laws with respect to these transfers.

6.2 Standard Contractual Clauses. With respect to any Personal Data transferred outside the European Economic Area, each party shall comply with its obligations under the Standard Contractual Clauses until such time as these clauses are repealed or updated by the European Commission or a supervisory authority established under Data Protection Laws. The Standard Contractual Clauses are subject to the terms and conditions of this DPA, including limitation of liability provisions, which provide business processes to aid the parties in such compliance as permitted by the Standard Contractual Clauses. Nothing in this DPA limits either party's liability, if any, to data subjects as provided under the Standard Contractual Clauses. Notwithstanding the Section below entitled "General", the Standard Contractual Clauses will be governed by the Data Protection Laws where Customer is established, as indicated by its address in the signature block above. **"Standard Contractual Clauses"** means the standard contractual clauses (controller to processor), attached as Exhibit B.

7. DATA SUBJECT REQUESTS. Optimizely has implemented technical and organisational measures to assist Customer with its obligation to respond to Data Subject requests under Data Protection Laws (currently documented here[3]). Optimizely will make this functionality available to Customer during Customer's Subscription Term. Customer agrees to follow Optimizely's documented procedures for Data Subject requests, confirm the requester's identity, provide sufficient information to identify relevant records containing Personal Data, review any records provided to Customer and otherwise cooperate with Optimizely's reasonable requests. Customer must not send duplicative or unnecessary requests to Optimizely (for example, requests for Personal Data not processed by the Optimizely Services). If Optimizely receives a Data Subject request identifying Customer, Optimizely will not respond directly unless required by law, and it will promptly forward that request to Customer.

8. BREACH NOTIFICATION. Unless prohibited by law, Optimizely must promptly (and without undue delay) notify Customer if it becomes aware of any Breach. The notice must include, as available: **(i)** a description of what happened; **(ii)** the scope of the Breach, including a description of the type of Personal Data involved; **(iii)** a description of the response; and **(iv)** other information as may be reasonably required to be disclosed under applicable Data Protection Laws. Optimizely will provide Customer with any other cooperation and assistance that Customer may reasonably require in relation to investigating and responding to the Breach. Optimizely may delay its notifications as requested by law enforcement or in light of its legitimate need to investigate or remediate a Breach. For security reasons, the parties agree to keep information regarding the Breach confidential, unless a disclosure is required by law or is made to an Affiliate or professional adviser who needs to know the information and is subject to a duty of confidentiality. Optimizely's obligation to report or respond to a Breach under this Section is not an acknowledgement by Optimizely of any fault or liability with respect to the Breach.

9. DATA DELETION. On the expiration or termination of the Governing Agreement, at Customer's request and after permitting Customer to download available personal data for up to 30 days following expiration or termination, Optimizely will delete Customer's Personal Data from its production systems unless applicable law or legal process prevents it from doing so.

10. AUDITS AND ASSISTANCE.

10.1 Assistance. Optimizely will provide Customer with commercially reasonable information and assistance, taking into account the nature of processing and the information available to Optimizely as a data processor, to help Customer comply with its obligations under GDPR Articles 32 to 36 with respect to processing of Personal Data under this DPA. As of the date of this DPA, Optimizely participates in the Cloud Security Alliance STAR self-assessment program and has completed the

[2] https://www.optimizely.com/legal/subprocessors/

[3] https://help.optimizely.com/Account_Settings/Request_or_delete_records_for_EU_General_Data_Protection_Regulation_(GDPR)

associated Consensus Assessments Initiative Questionnaire (CAIQ), currently available here[4].

10.2 Audits. Customer may request that Optimizely make available documentation that is reasonably necessary to demonstrate compliance with this DPA and the obligations under GDPR Article 28, including the executive summary of Optimizely's annual security audit conducted by an independent, third party auditor. Without limiting Customer's responsibilities under this DPA, Optimizely will use reasonable efforts to inform Customer if it discovers, in connection with its obligations under GDPR Article 28(3)(h), information that in Optimizely's opinion would cause Customer's Instructions to infringe Data Protection Laws. Except with respect to audits required by a government regulator or supervisory authority, Customer agrees to exercise its audit rights under applicable Data Protection Laws as specified in this Section.

10.3 Government Requests. Optimizely will provide Customer with reasonable access to its documentation and systems in the event of an audit required by a government regulator or supervisory authority for compliance with Data Protection Laws. Further, each party may process Personal Data where required in response to court or government agency requests or by applicable law. Unless prohibited by law, Optimizely will promptly inform Customer if a court, regulator, government agency or supervisory authority demands access to Personal Data.

10.4 Other Provisions. The parties will mutually agree on the timing and scope of any requests and audits under this Section, which will be: **(i)** carried out in such a way as to not disrupt Optimizely's business; **(ii)** performed no more than once per calendar year (unless otherwise required by government regulator or supervisory authority) and at Customer's sole expense, including reimbursement for Optimizely's time spent on any on-site audit; and **(iii)** subject to reasonable confidentiality protections requested by Optimizely. Any executive summaries, audit reports or other information obtained by Customer will be considered Optimizely's Confidential information.

11. TERM AND TERMINATION. This DPA is effective as of the Data Processing Addendum Effective Date and continues in effect until termination or expiration of the Governing Agreement. Either party has the right to terminate this DPA and the Governing Agreement if: **(i)** the parties agree in writing that this DPA conflicts with currently applicable Data Protection Laws, including as a result of an amendment or change in applicable law; **(ii)** any authority or court demands or requests changes to these agreements and the parties cannot agree on adequate amendments to reflect these changes; or **(iii)** Optimizely notifies Customer in writing that it can no longer meet its obligations under applicable Data Protection Laws.

12. GENERAL. If Customer and Optimizely have signed a prior data processing agreement, that agreement is terminated and replaced by this DPA as of the DPA Effective Date above. If any of Customer's Affiliates is considered the data controller (either alone or jointly with Customer) of Personal Data, Customer is responsible under this DPA for this Personal Data and Affiliate. This DPA is incorporated as an attachment to the Governing Agreement. It is subject to all the terms and conditions of that agreement, including provisions related to limitations of liability, termination, jurisdiction and governing law. However, this DPA will control with respect to how Optimizely will process Customer's Personal Data.

13. DEFINITIONS.

13.1 "Affiliate" means any entity which is controlled by, in control of, or is under common control with a party to this Agreement, where "control" means either the power to direct the management or affairs of the entity or ownership of 50% or more of the voting securities of the entity.

13.2"Breach" means a security breach of Optimizely's systems that has resulted in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data transmitted, stored or otherwise processed by Optimizely.

13.3"Data Subject" means an identified or identifiable natural person as defined under Data Protection Laws.

13.4"Personal Data" means personal data (as defined under Data Protection Laws) provided by Customer to the Optimizely Service concerning Data Subjects in the European Economic Area, Switzerland, and the United Kingdom.

13.5"Data Protection Laws" means the General Data Protection Regulation (Regulation (EU) 2016/679) (**"GDPR"**) and the national laws of Switzerland and the United Kingdom relating to protection of Personal Data.

13.6 "Instructions" means Customer's instructions to Optimizely: (i) to provide the Optimizely Service to Customer in accordance with the features and functionalities of the Optimizely Service and related Documentation; (ii) through the Authorized User-initiated actions on and through the Optimizely Service, or otherwise based on Customer's configuration and use of the Optimizely Service; (iii) contained in the Governing Agreement and/or any applicable Order Form; and (iv) mutually agreed by the parties in writing.

13.7"Experimentation Service Terms" means the "Experimentation Service" as defined in the Agreement.

[4] https://cloudsecurityalliance.org/star/registry/optimizely/

EXHIBIT A TO DPA

Data controller: The data controller is:

- Customer, a company using the Optimizely Services (as that term is defined in the DPA).

Data processor: The data processor is:

- Optimizely, a provider of digital experimentation, personalization, testing and experience optimization services through a SaaS platform.

Data subjects: The personal data transferred concern the following categories of data subjects (please specify):

- visitors to Customer's websites and apps ("**Visitors**").
- Customer's employees and other personnel who create accounts to use the Optimizely Services ("**Customer End Users**").

Categories of data: Personal Data processed by Optimizely on Customer's behalf may include the following categories of data:

- *Visitors:* IP addresses, random unique identifiers such as cookie IDs or similar identifiers, and experiment and event data associated with these identifiers (such as device type, variation and experiment IDs, browser and OS version and the elements of the site being tested) based on Customer's use and configuration of the Optimizely Service. Customer may take advantage of features of the Optimizely Service such as IP address anonymization to minimize collection of such data and must comply with any prohibitions in the Governing Agreement relating to restrictions on collection and use of Personal Data.
- *Customer End Users:* Names, email addresses, passwords, contact details, and similar Personal Data provided by Customer End Users when creating an Optimizely account.

Special categories of data (if appropriate): The personal data transferred concern the following special categories of data (please specify):

- Not applicable.

Processing operations: The personal data transferred will be subject to the following basic processing activities (please specify):

- Optimizely will provide the feature flagging, personalization, analytics and/or other Optimizely Services ordered by Customer according to the Instructions (as that term is defined in the DPA). Optimizely will also provide Customer End Users with reporting, communications and other features offered by Optimizely.

Description of the technical and organisational security measures:

- As described in the Section of the DPA above entitled Security Measures.

List of authorized sub-processors:

- As specified at https://www.optimizely.com/legal/subprocessors.

<u>EXHIBIT B TO DPA</u>

Standard Contractual Clauses (controller to processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: *The entity identified as the "Customer" in the Data Processing Addendum signed in connection with these clauses ("DPA").*

Address: *As specified in the DPA*

Tel.: *As specified in the DPA*

fax:

e-mail: *As specified in the DPA*

Other information needed to identify the organisation: –

(**the data exporter**)

And

Name of the data importing organisation: *Optimizely, Inc.*

Address: *631 Howard Street, Suite 100, San Francisco CA 94105, United States*

Tel.: *US: +1-800-252-9480* | *DE: +49 (0)221 828 297 24* |*NL: +31 (0)20 26 100 60;*

fax: N/A;

e-mail: *privacy@optimizely.com*

Other information needed to identify the organisation: –

(**the data importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in *Appendix 1*.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[5];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the

[5] *Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.*

data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[6]

The data importer agrees and warrants:

[6] *Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the*

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely: *as specified in the DPA.*

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[7]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely: *as specified in the DPA*.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

[7] *This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.*

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

- *See DPA Exhibit A*

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

- *See DPA Exhibit A*

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

- *See DPA Exhibit A*

Categories of data

The personal data transferred concern the following categories of data (please specify):

- *See DPA Exhibit A*

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

- *See DPA Exhibit A*

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

- *See DPA Exhibit A*

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

- *See DPA Exhibit A*

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

List of authorized sub-processors according to Clause 11:

- *See DPA Exhibit A*