DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is integrated into the Master Services Agreement ("**MSA**") entered into by and between you and/or the entity you represent ("**Customer**") and LogicLoop ("**Service Provider**"), each a "**party**" and together the "**parties**." Except to the extent otherwise expressly set forth in this DPA, this DPA is governed by the terms and conditions of the MSA available at https://docs.logicloop.com/security-and-legal/terms-of-use, or if applicable, the MSA entered into between the Service Provider and the Customer. Any capitalized defined terms not otherwise defined herein shall have the meanings set forth in the MSA. In the event of any inconsistency or conflict between this DPA and the MSA, the DPA applies. This Addendum is effective as of the date of Customer's first use of the services or, if applicable, the date of the MSA.

1. Definitions.

a. "**Applicable Data Protection Law**" means any applicable laws, rules, regulations, self-regulatory guidelines, implementing legislation, or third party terms relating to privacy, security, data protection, or confidentiality, including, as applicable (i) the California Consumer Privacy Act of 2018 California Civil Code § 1798.100 et seq. ("**CCPA**"); (ii) the UK Data Protection Act 2018; and (iii) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**GDPR**").

b. "**Customer Confidential Information**" has the meaning set out in the MSA. For avoidance of doubt, Customer Confidential Information includes Personal Information.

b. "**controller**," "**business**," "**processor**," "**service provider**," "**data subject**," "**consumer**," "**process**," "**sell**," "**commercial purpose**," and "**supervisory authority**" (or any equivalent terms) have the meaning set out under Applicable Data Protection Law.

c. "**EU Model Clauses**" means the standard contractual clauses annexed to the EU Commission Decision 2010/87/EU of February 5, 2010 for the Transfer of Personal Information to Processors established in Third Countries under the Directive 95/46/EC, or any successor standard contractual clauses that may be adopted pursuant to an EU Commission decision.

d. "**Personal Information**" means information that is processed by Service Provider on behalf of Customer and that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer, data subject, or household or is defined as "personal information," "personal data", "personally identifiable information," or similar term under Applicable Data Protection Law.

e. "**Subprocessor**" means any subcontractor of Service Provider that has access to Customer Confidential Information in connection with Customer's use of the Services.

2. Processing of Customer Confidential Information.

a. The parties acknowledge and agree that Service Provider will have access to Customer Confidential Information in connection with Customer's use of the Services. Customer is the controller or business that determines the purposes for and the manner in which Customer Confidential Information is processed by Service Provider, and Service Provider is the processor

or service provider that processes Customer Confidential Information according to Customer's instructions.

b. Customer hereby instructs Service Provider to process Customer Confidential Information solely for the purposes of (i) providing the Services in accordance with the MSA; and (ii) complying with Customer's documented written instructions. Service Provider agrees that it will not process Customer Confidential Information for any other purpose. If Service Provider must process Customer Confidential Information as otherwise required by Applicable Data Protection Law, Service Provider shall inform Customer of that legal requirement before processing Customer Confidential Information, unless that law prohibits such disclosure on important grounds of public interest. Service Provider shall comply with all Applicable Data Protection Laws, and shall not cause Customer to violate any Applicable Data Protection Laws.

c. Service Provider shall process Personal Information according to the following specifications:

i. The subject matter of the processing is the performance of the Services pursuant to the MSA.

ii. The duration of the processing is for the duration of this MSA except where otherwise required by Applicable Data Protection Law.

iii. The categories of individuals, consumers, or data subjects whose Personal Information may be processed in performing the Services include, Customer's personnel, representatives, contractors, partners, end users, and persons of interest.

iv. The types of Personal Information are determined and controlled by Customer, in Customer's discretion, and may include, name, email address, phone number, IP address, Ad ID, username, and password.

d. Service Provider shall not: (i) sell Customer Confidential Information; (ii) retain, use, or disclose Customer Confidential Information for any purpose other than for the specific purpose of performing the Services; (iii) retain, use, or disclose Customer Confidential Information for a commercial purpose other than providing the Services; or (iv) retain, use, or disclose Customer Confidential Information outside of the direct business relationship between Service Provider and Customer. Service Provider certifies that it understands these restrictions and will comply with them.

3. Subprocessors. Service Provider shall not disclose or otherwise make available Customer Confidential Information to anyone without: (a) notifying Customer of the anticipated disclosure (so as to provide Customer the opportunity to oppose the disclosure and obtain a protective order or seek other relief); (b) obtaining Customer's prior written consent to the disclosure; (c) conducting a reasonable investigation of the recipient's safeguards to ensure such safeguards are reasonable and consistent with Service Provider's obligations under the MSA; and (d) contractually imposing upon the third party the same or substantially similar contractual duties imposed on Service Provider and rights provided to Customer as in the MSA. Customer provides specific written authorization for the use by Service Provider of the Subprocessors identified in Schedule 1. Service Provider will inform Customer of any intended changes concerning the addition or replacement of Sub-Processors and Customer will have an opportunity to object to such changes on reasonable grounds within seven business days after being notified. If the parties are unable to resolve such objection, either party may terminate the MSA by providing written notice to the other party. Service Provider shall be liable for the acts and omissions of its Subprocessors to the same extent it would be liable if performing the services of each Subprocessor directly under the terms of the MSA.

4. Security. Service Provider shall implement and maintain reasonable and appropriate technical and organizational measures to ensure the protection, confidentiality, and integrity of Customer Confidential Information. The minimum technical and organizational measures to be implemented by Service Provider are set forth in Schedule 2. Service Provider shall regularly monitor compliance with these measures, and shall not materially decrease them for as long as it processes Customer Confidential Information. Service Provider shall ensure that persons authorized to carry out processing have committed themselves to confidentiality or are under the appropriate statutory obligation of confidentiality. Service Provider shall preserve Customer Confidential Information in accordance with Customer instructions and requests, including any retention schedules and/or litigation hold orders provided by Customer to Service Provider, independent of where the Customer Confidential Information is stored.

5. Security Incidents. Service Provider shall implement and maintain reasonable and appropriate security incident management policies and procedures for responding to any actual or reasonably suspected accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, or access to Customer Confidential Information ("**Security Incident**"). In the event of a Security Incident, Service Provider shall, at its own expense: (a) provide prompt notice to Customer (no more than twenty-four (24) hours) upon discovery of the Security Incident; (b) use commercially reasonable efforts to prevent, contain, and mitigate the impact of the Security Incident; (c) collect, preserve, and document all evidence concerning the discovery, cause, vulnerability, remedial actions and impact related to such Security Incident, which shall meet reasonable expectations of forensic admissibility; and (d) reasonably cooperate with Customer and its designees for purposes of Security Incident response, including if requested by Customer, providing notice to individuals or entities whose Personal Information was or may have been affected in a manner and format specified by Customer. The content of any filings, communications, notices, press releases or reports related to any Security Incident must be approved by Customer prior to any publication or communication thereof unless prohibited by law. Service Provider shall reimburse Customer on demand for all costs incurred by Customer arising out of or in connection with any such Security Incident.

6. Requests and Assistance. Service Provider shall, to the extent legally permitted, promptly notify Customer if Service Provider receives a request from an individual, consumer, or data subject to exercise their rights under Applicable Data Protection Law or receives a request or complaint from a supervisory authority or anyone else ("**Request**"). Taking into account the nature of the processing, Service Provider shall assist Customer in the fulfilment of Customer's obligation to respond to the Request, and shall not respond to the Request without written approval from Customer. Upon request by Customer, Service Provider shall assist Customer as necessary to carry out data protection impact assessments related to Customer's use of the Services, and in the cooperation or prior consultation with supervisory authorities in the performance of Service Provider's tasks relating to the data protection impact assessments.

7. Return and Destruction. Service Provider shall return or destroy all Customer Confidential Information (such that Customer Confidential Information is rendered unusable and unreadable) at Customer's written request, when such Customer Confidential Information is no longer needed to perform the Services, or thirty (30) days following termination of the MSA. Service Provider shall destroy all existing copies unless applicable law requires retention of the Customer Confidential Information, in which case Service Provider shall inform Customer of the applicable law and retained data and not process the Customer Confidential Information except as necessary to comply with the applicable law. Upon request by Customer, Service Provider shall provide written certification that all such Customer Confidential Information has been returned or deleted.

8. Cross-Border Data Transfers. Service Provider shall not transfer or cause to be transferred any Customer Confidential Information from one jurisdiction to another jurisdiction without Customer's prior written consent, and where Customer has consented to such transfer, the transfer

will be in accordance with Applicable Data Protection Law and will not cause Customer to be in breach of Applicable Data Protection Law. To the extent Personal Information is collected in the United Kingdom or European Union, Customer and Service Provider hereby enter into the standard contractual clauses as attached hereto as Schedule 3.

9. Audit. Upon provision of reasonable notice to Service Provider, once per year as long as Service Provider processes Customer Confidential Information, Customer may undertake an assessment by a third party auditor at Customer's expense, an audit of Service Provider's compliance with this DPA. In addition, Service Provider shall conduct a comprehensive independent third party audit of its privacy and data security measures at least once per year as long as Service Provider processes Customer Confidential Information and provide such audit findings to Customer. Service Provider shall promptly implement any required safeguards as identified by a third party auditor or Customer and/or as is necessary for Service Provider to fully comply with the MSA.

10. Material Breach and Indemnification. The following shall be considered Service Provider's material breach of the MSA: Servicer Provider's (or its Subprocessors') failure to comply with any of its obligations set forth in this DPA. In addition to any indemnification obligations elsewhere in the MSA, Service Provider agrees to indemnify, defend, and hold harmless Customer and its affiliates, subsidiaries, successors and assigns (and their officers, directors, employees, sublicensees, customers and agents) from and against any and all claims, losses, demands, liabilities, damages, settlements, expenses and costs (including attorneys' fees and costs), arising from, in connection with, or based on allegations of, Service Provider's (or its Subprocessors') failure to comply with any of its obligations set forth in this DPA. This indemnification obligation is not subject to any limitation of liability elsewhere in the MSA.

Schedule 1

Subprocessors

Customer approves Service Provider's use of the following subprocessors for the processing of Customer Confidential Information:

AWS, Slack, Zendesk, Google workspace

Schedule 2

Minimum Technical and Organization Measures

A. Service Provider has implemented and will maintain reasonable and appropriate technical and organizational measures to protect Customer Confidential Information against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, and procedures and internal controls set forth in this Schedule 2.

B. More specifically, Service Provider's security program shall include, at a minimum:

Access Control of Processing Areas

Service Provider has implemented and will maintain reasonable and appropriate measures to prevent unauthorized access to the data processing equipment (namely telephones, database and application servers and related hardware) where Customer Confidential Information is processed or used, including:

- establishing security areas and physical controls;
- protection and restriction of access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- all access to the data center where Customer Confidential Information are hosted is logged, monitored, and tracked; and
- the data center where Customer Confidential Information are hosted is secured by a security alarm system, and other appropriate security measures.

Access Control to Data Processing Systems

Service Provider has implemented and will maintain reasonable and appropriate measures to prevent data processing systems where Customer Confidential Information is processed and used from being used by unauthorized persons, including:

- use of industry best encryption technologies, including for data at rest and in-transit;
- identification of the terminal and/or the terminal user to Service Provider and processing systems;
- automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and
- all access to data content is logged, monitored, and tracked.

Access Control to Use Specific Areas of Data Processing Systems

Service Provider commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that Customer Confidential Information cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the Customer Confidential Information;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;

- monitoring capability in respect of individuals who delete, add or modify the Customer Confidential Information;
- release of data only to authorized persons, including allocation of differentiated access rights and roles;
- use of industry standard encryption technologies, including for data at rest and in-transit; and
- control of files, controlled and documented destruction of data.

Availability Control

Service Provider has implemented and will maintain reasonable and appropriate measures to ensure that Customer Confidential Information is protected from accidental destruction or loss, including:

- infrastructure redundancy; and
- backup is stored at an alternative site and available for restore in case of failure of the primary system.

Transmission Control

Service Provider has implemented and will maintain reasonable and appropriate measures to prevent Customer Confidential Information from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of industry standard firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- Highly confidential employee data is encrypted within the system;
- providing user alert upon incomplete transfer of data (end to end check); and
- as far as possible, all data transmissions are logged, monitored and tracked.

Input Control

Service Provider has implemented and will maintain reasonable and appropriate input control measures, including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of unique authentication credentials or codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- automatic log-off of user ID's that have not been used for a substantial period of time; and
- proof established within Service Provider’s organization of the input authorization; and
- electronic recording of entries.

Separation of Processing for different Purposes

Service Provider has implemented and will maintain reasonable and appropriate measures to ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users;
- modules within Service Provider’s data base separate which data is used for which purpose, i.e. by functionality and function;

- at the database level, data is stored in different normalized tables, separated per module, or function they support; and
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Documentation

Service Provider will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Service Provider will ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Schedule 2.

Monitoring

Service Provider has implemented and will maintain reasonable and appropriate measures to monitor access restrictions to Service Provider's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- individual appointment of system administrators;
- adoption of commercially reasonable and appropriate measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by Service Provider and Applicable Data Protection Law; and
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to data exporter upon request.

Limits on Retention/Destruction

- Service Provider will destroy or dispose of records containing Customer Confidential Information when there no longer exists any lawful basis for processing. Service Provider has implemented and will maintain reasonable and appropriate measures to securely destroy all Customer Confidential Information consistent with Applicable Data Protection Law. Methods of performing these actions may include the use of a third party disk scrubbing utility or destruction of the drive, such as by degaussing, shredding, or other means of physically destroying data through specialized equipment and services.

Schedule 3

Standard Contractual Clauses (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

The entity identified as "Customer" in the DPA (the "data exporter**"**)

and

The entity identified as "Service Provider" in the DPA (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;

(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 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

The data importer agrees and warrants:

(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.

   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.

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. 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.

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.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties. By signing the DPA, the parties will be deemed to have signed this Appendix 1.

Data exporter
The data exporter is the entity identified as "Customer" in the DPA.

Data importer
The data importer is the entity identified as "Service Provider" in the DPA.

Data subjects
Data subjects include the data exporter's personnel, representatives, contractors, partners, end users, and persons of interest.

Categories of data
The personal data relating to individuals which is processed by the data importer through the data exporter's use of its services. The data exporter determines the types of data per each service used.

Processing operations
The personal data transferred will be subject to the processing activities required for performance of the services by data importer pursuant to the MSA.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties. By signing the DPA, the parties will be deemed to have signed this Appendix 2.

The details of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(c) and 5(c) are set out in Schedule 2 to the DPA.