Data Processing Agreement

This Data Processing Agreement (**"DPA"**) is made between Gen Digital Inc. and its affiliates as identified in any Order (**"Gen"**) and the seller or provider of any Solutions as identified in such Order (**"Provider"**).

Gen and Provider are each a **"Party"** or the **"Parties"** to this DPA.

WHEREAS in this context:

Gen has procured from Provider certain products and/or services under the Gen Master Purchase Agreement (the **"MPA"**) that requires the processing of Personal Data. This DPA is supplemental to the MPA and sets out the terms that apply to the extent that the Provider Processes or causes to be Processed any Personal Data

The Parties agree as follows:

1. **Definitions**. Capitalized terms used in this DPA and not otherwise defined in this DPA will shall have the meaning as ascribed to them in the MPA. If any definitions in the MPA or this DPA conflict with statutory definitions provided in any Data Protection Law, the definition in the applicable Data Protection Law shall control.

"Business" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the thresholds set out in the CCPA.

"California Personal Data" means the Gen Personal Data the Processing of which is subject to the CCPA.

"CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 es seq., as amended, in particular, by the California Privacy Rights Act of 2020.

"Controller" means the party which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"Data Protection Law" means the EU Data Protection Law, the CCPA, the UK GDPR, the Swiss Data Protection Law and any other data protection laws which may be applicable to the Personal Data Processed under the MPA.

"Deidentified Information" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the Business that possesses the information: (i) takes reasonable measures to ensure that the information cannot be associated with a consumer or household, (ii) publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision, and (iii) contractually obligates any recipients of the information to comply with all provisions under the CPPA and Section 11.6 of this DPA.

“EEA” means the European Economic Area.

"EU Data Protection Law” means (i) the General Data Protection 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 for the transfer of personal data to a third country (**“GDPR”**) and (ii) any applicable data protection laws of any EEA member state.

“EU Personal Data” means the Gen Personal Data the Processing of which is subject to the EU Data Protection Law.

“Gen Personal Data” means Personal Data that the Provider Processes under the MPA.

“Personal Data” means any information related to any identified or identifiable natural person (“**Data Subject**”), an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, or as defined by the Data Protection Law.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

“Process” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means a natural or legal person, public authority, agency, or other body which Processes personal data on behalf of the Controller.

“**Service Provider**” means a person that processes personal information on behalf of a Business that receives from or on behalf of the Business a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract meets the requirements of the CCPA.

“Services” means the services as described in MPA.

“Standard Contractual Clauses” are as defined in Section 10.2 of this DPA.

“**Swiss Data Protection Law**” means the Swiss Federal Act on Data Protection.

“**Swiss Personal Data**” means the Gen Personal Data the Processing of which is subject to the Swiss Data Protection Law.

“**UK GDPR**” means the General Data Protection 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 for the transfer of personal data to a third country as it forms part of the law of England and Wales.

"**UK Personal Data**" means the Gen Personal Data the Processing of which is subject to the UK GDPR.

2. Subject of the DPA

2.1. With respect to Processing of Gen Personal Data in connection with the MPA, Gen shall act as the Controller and Provider as the Processor.

2.2. Detailed specification of Gen Personal Data Processed, including the subject-matter, the nature and purpose of the Processing, the type of personal data and categories of data subjects are provided in the Order.

2.3. The subject-matter of the Processing of Personal Data is the provision of Services under the MPA.

2.4. The nature of the Processing of Personal data may include but is not limited to: collection, recording, organization, storage, use, disclosure, erasure, augmentation, enrichment and transmission in connection with provision of the Services.

3. Compliance with Laws and Processing Instructions.

3.1. Each Party will comply with the Data Protection Law as applicable to it. To the extent required by any Data Protection Law, the Parties agree to negotiate in good faith and execute any such additional, supplemental or revised documents pertaining to the Processing of Gen Personal Data as reasonably necessary for the provision of Services under the MPA.

3.2. The Provider shall Process the Gen Personal Data only on documented instructions from Gen, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so under applicable Data Protection Law; in such case, the Provider shall inform Gen of that legal requirement before Processing of the Gen Personal Data, unless that law prohibits such information on important grounds of public interest. Provider shall immediately inform Gen if, in its opinion, an instruction infringes on any Data Protection Law.

3.3. Provider shall Process Gen Personal Data solely for the purposes set out in the MPA and cannot Process Gen Personal Data for any other purposes to be determined by the Provider.

3.4. With respect to Processing of Gen Personal Data, the Provider may only use such employees, members of its corporate bodies or other similar persons who are sufficiently trained, familiar with all the Gen's instructions and Provider's internal guidelines.

3.5. The Provider shall Process Gen Personal Data for as long as it is necessary to fulfill its obligations under Gen´s instructions. After the termination or expiry of the MPA, the Provider shall, without undue delay, destroy or remove all Gen Personal Data that it has not returned Gen. This does not apply if the Provider has legitimate reasons to further Process Gen Personal Data under Data Protection Law.

4. Security

4.1. The Provider hereby represents and warrants to Gen that it has implemented appropriate technical and organizational measures to ensure the security of the Gen Personal Data, including protection against a breach of security leading to a Personal Data Breach. In particular, the Provider hereby represents and warrants that it has, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including (i) internal policies and practices for protection of Personal Data, including for training and supervision of its staff, especially where cross-border transfers and Processing are concerned, and (ii) the technical and organizational measures explicitly specified in the MPA. The Provider shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

4.2. The Provider shall encrypt the Gen Personal Data and shall (i) keep the encryption key separately from the Gen Personal Data and (ii) not provide to any public authority an encryption key to the Gen Personal Data or assist the public authority in any other way in obtaining the Gen Personal Data, unless required to do so by applicable law.

4.3. The Provider shall grant access to the Gen Personal Data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the MPA. It shall ensure that persons authorized to Process the Gen Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Personal Data Breach Notification and Remediation.

5.1. Provider will promptly, but not later than 24 hours from becoming aware of the Personal Data Breach, notify Gen of the occurrence or possible occurrence of the Personal Data Breach affecting Gen Personal Data. Provider shall send all notifications of Personal Data Breaches to: security@gendigital.com. Such notification shall contain, at least: (i) description of the nature of the Personal Data Breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned); (ii) its likely consequences and the measures taken or proposed to be taken to address the Personal Data Breach, including to mitigate its possible adverse effects; and (iii) the details of a contact point where more information concerning the Personal Data Breach can be obtained.

5.2. In case of the Personal Data Breach, the Provider shall provide reasonable cooperation to Gen in informing the affected Data Subjects.

5.3. Except and only to the extent expressly required by law, Provider agrees that it will not inform any third party that Gen Personal Data has been involved in a Personal Data Breach without Gen's prior written consent. If Provider is compelled by law to provide public/third-party notification of a Personal Data Breach, Provider will not identity Gen (directly or indirectly) and will use commercially reasonable efforts to obtain Gen's prior approval regarding the content of such disclosure to minimize any adverse impact to Gen, and its respective customers and/or employees.

6. Processing carried out by other persons

6.1. Gen generally authorizes the Provider to engage other Processors (sub-processors) listed in the Order. The Provider shall inform Gen of any intended changes concerning the addition or replacement of sub-processors together with the information necessary for Gen to assess the sub-processor in question without undue delay (at least 30 business days prior to the engagement of the sub-processor in question), thereby giving Gen the opportunity to object to such changes. If Gen does not object to changes in sub-processors within 30 business days of the receipt of the notification of change, the change is considered as approved. A list of sub-processors approved by Gen as at the date of this DPA is included in the Order.

6.2. In relation to the Processing of Gen Personal Data, the sub-processors shall maintain confidentiality, i.e. they shall not disclose the Gen Personal Data or make it available to any other person without Gen's consent. This does not apply to the legal obligation to disclose Personal Data to entities authorized to receive such data by law. The confidentiality obligation is not limited and shall apply even after termination of the MPA.

6.3. The Provider shall ensure by way of a contract that sub-processors comply with the obligations to which the Provider is subject pursuant to the DPA and under Data Protection Law. At Gen's request, the Provider shall provide a copy of its sub-processor agreements and any subsequent amendments to Gen. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the Provider may redact the text of the sub-processor agreements prior to sharing the copy.

6.4. The Provider shall remain fully responsible to Gen for the performance of the sub-processor's obligations in accordance with the DPA. The Provider shall notify Gen, without undue delay, of any failure by the sub-processor to fulfil its contractual obligations.

6.5. The Provider shall agree a third party beneficiary clause with the sub-processor whereby - in the event the Provider has factually disappeared, ceased to exist in law or has become insolvent - Gen shall have the right to terminate the sub-processor agreement and to instruct the sub-processor to erase or return the Gen Personal Data.

7. Cooperation and assistance

7.1. The Provider shall deal promptly and adequately with inquiries from Gen about the Processing of Gen Personal Data in accordance with this DPA and provide Gen with the necessary assistance to comply with the applicable Data Protection Law, in particular:

(a) with the handling of Data Subjects´ requests; and

(b) when carrying out data protection impact assessment and consulting with the data protection authorities.

7.2. In case the Provider receives a Data Subjects´ request relating to the Gen Personal Data Processed under the MPA, the Provider shall promptly, but not later than within two business days, forward such request to Gen. The Provider shall not respond to such a request without Gen's prior written consent.

8. Control and audit

8.1. The Provider is obliged to allow Gen to check the Provider's compliance with all obligations under this DPA and Data Protection Law.

8.2. The Provider shall upon Gen´s request, without undue delay, submit documents proving that the Provider Processes Gen Personal Data in accordance with this DPA and Data Protection Law and enable the audit to be carried out by Gen or a person authorized by it to perform it. Gen shall notify the Provider about its intent to perform an audit reasonably in advance.

8.3. If a control or an audit is carried out at the Provider´s place by public authorities, the Provider shall immediately notify Gen about such control or audit and provide relevant documents, unless prohibited from doing so under applicable law.

9. International Transfers of Personal Data

Provider and its sub-processors shall only transfer Gen Personal Data from its country of origin in accordance with the Data Protection Law.

10. Additional Provisions Applicable to the EU Personal Data

10.1. The provisions set out in this Section 10 shall only apply to Processing of the EU Personal Data.

10.2. Any transfer of EU Personal Data by the Provider to a third country (in the sense of the GDPR) shall be governed by the standard contractual clauses attached as Schedule 1 to this DPA (the **"Standard Contractual Clauses"**).

10.3. The Provider confirms that it is not an electronic communication service provider pursuant to the US Foreign Intelligence Surveillance Amendments Act of 2008 **("FISA"**) or subject to any other similar legislation of any country outside the EEA that imposes requirements for disclosure of Personal Data to public authorities or grants such public authorities powers of access to Personal Data (for example, for criminal law enforcement purposes, regulatory oversight or national security) which restrict the fundamental rights of Data Subjects (including by failing to provide adequate redress by a judicial or other independent authority) and which go beyond what is necessary and proportionate in a democratic society to secure important legitimate aims such as such those listed in Article 23 (1) of the GDPR (defense, combating criminal and other unlawful activities, etc.).

10.4. The Provider confirms that, in the last three years before the execution of the MPA, it has not disclosed to any public authority any Personal Data required by this public authority for national security reasons, including under Section 702 of the FISA.

11. Additional Provisions Applicable to the California Personal Data

11.1. The provisions set out in this Section 11 shall only apply to Processing of the California Personal Data.

11.2. Roles and Scope.

(a) This DPA applies only to the collection, retention, use, disclosure, and sale or sharing, as the case may be, of Personal Data provided by Gen to, or which is Collected on behalf of Gen by, Provider to provide Services to Gen pursuant to the MPA or to perform a business purpose.

(b) The Parties acknowledge and agree that Gen is a Business and appoints Provider as a Service Provider to Process Personal Data on its behalf and at its direction.

11.3. Restrictions on Processing.

Except as otherwise permitted by the CCPA, Provider is prohibited from:

(a) selling or sharing the Personal Data;

(b) retaining, using, or disclosing Personal Data for any purpose, including any commercial purpose, other than for the specific purpose of performing the Services specified in the MPA entered into with Gen, as set out in this DPA;

(c) retaining, using, or disclosing Personal Data outside of the direct business relationship between Provider and Gen; or

(d) Combining the Personal Data that the Provider receives from, or on behalf of, another person or persons, or collects from its own interaction with a consumer, with the Personal Data received from or on behalf of Gen hereunder.

11.4. Upon direction by Gen, and in any event no later than 30 days after receipt of a request from Gen, Provider shall promptly delete Personal Data as directed by Gen.

11.5. Provider shall not be required to delete any Personal Data to comply with a Consumer’s request directed by Gen if it is necessary to maintain such information in accordance with the CCPA, in which case Provider shall promptly inform Gen of the exceptions relied upon to retain Personal Data. Provider shall not use Personal Data retained for any other purpose than provided for by that exception.

11.6. Deidentified Information.

In the event that any Party shares Deidentified Information with another Party, the receiving Party warrants that it: (i) has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain; (ii) has implemented business processes that specifically prohibit reidentification of the information; (iii) has implemented business processes to prevent inadvertent release of Deidentified Information; and (iv) will make no attempt to reidentify the information.

11.7. No Sale of Information. The Parties acknowledge and agree that the exchange of Personal Information between the Parties does not form part of any monetary or other valuable consideration exchanged between the Parties with respect to the MPA.

12. <u>Additional Provisions Applicable to UK Personal Data</u>

12.1. The provisions set out in this Section 12 shall only apply to Processing of the UK Personal Data.

12.2. Any transfer of the UK Personal Data by the Provider to a third country (in the sense of the UK GDPR) shall be governed by the Standard Contractual Clauses attached as Schedule 1 to this

DPA as supplemented by template Addendum B.1.0 issued by the Information Commissioner 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 (the **"UK Approved Addendum"**) and Part 1 of the UK Approved Addendum shall be populated as set out below:

- Table 1. The "start date" will be the date this DPA enters into force. The "Parties" are Gen as exporter and the Provider as importer.

- Table 2. The "Addendum EU SCCs" are the modules and clauses of the Standard Contractual Clauses in Commission Implementing Decision (EU) 2021/914, including the text from module two and three of such clauses and not including any clauses marked as optional.

- Table 3. The "Appendix Information" is as set out in this DPA and Order.

- Table 4. The exporter may end the UK Approved Addendum in accordance with its Section 19.

12.3. In the event that: (1) the UK Approved Addendum is no longer valid for use under Article 46 of the UK GDPR; and (2) the Information Commissioner issues standard data protection clauses under s.119A(1) of the UK Data Protection Act 2018 which incorporate and modify the EU Standard Contractual Clauses to be effective under the laws of the United Kingdom (**"New UK Standard Contractual Clauses"**), then the Parties agree that the New UK Standard Contractual Clauses shall apply to any transfer of the UK Personal Data by the Provider to a third country (in the sense of the UK GDPR) from such date as Gen notifies Provider, with the details of the Parties, Annexes and modules as specified in this DPA in relation to the EU Standard Contractual Clauses. The Parties agree that Gen may, by notice to the Provider, make any further amendments to the application of the New UK Standard Contractual Clauses as Gen deems reasonably necessary to implement such replacement standard contractual clauses.

13. <u>Additional Provisions Applicable to Swiss Personal Data</u>

13.1. The provisions set out in this Section 13 shall only apply to Processing of the Swiss Personal Data.

13.2. Any transfer of the Swiss Personal Data by the Provider to a third country (in the sense of the Swiss Data Protection Law) shall be governed by the Standard Contractual Clauses, provided that any references in the Standard Contractual Clauses to the GDPR shall refer to the Swiss Data Protection Law, the term 'member state' must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the clauses, and the clauses shall also protect the data of legal persons.

14. <u>Order of Precedence.</u>

If there is a conflict between the MPA and this DPA, the terms of this DPA will control including the terms of the Standard Contractual Clauses.

Schedule 1

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of 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 8.1(b), 8.9(a), (c), (d) and (e);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

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

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

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

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

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion.

The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

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

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

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

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

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

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

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

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

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

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

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

Clause 13

Supervision

(a) Where the data exporter is 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;

(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 laws 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 court

ANNEX I

PARTIES AND DESCRIPTION

A. LIST OF PARTIES

Data exporter(s):

Name, Address and Contact person's name, position and contact details: as set out in the Order.

Activities relevant to the data transferred under these Clauses: The relevant activities of the data exporter are as set out in the MPA.

Role: Controller.

Data importer(s):

Name, Address and Contact person's name, position and contact details: as set out in the Order.

Activities relevant to the data transferred under these Clauses: The relevant activities of the data importer are as set out in the MPA.

Role: Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As set out in the Order.

Categories of personal data transferred

As set out in the Order.

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.

As set out in the Order.

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

As set out in the Order.

Nature of the processing:

The nature of the processing of personal data may include but is not limited to: collection, recording, organization, storage, use, disclosure, erasure, augmentation, enrichment and transmission in connection with provision of the Services.

Purpose(s) of the data transfer and further processing

The importer will process personal data for the purposes of providing the Services under the MPA.

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

The importer shall process personal data for as long as it is necessary to fulfill its obligations under exporter´s instructions. After the termination or expiry of the MPA, the importer shall, without undue delay, destroy or remove all personal data that it has not returned importer. This does not apply if the exporter has legitimate reasons to further process personal data under data protection law.

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

As set out in the Order.

C. COMPETENT SUPERVISORY AUTHORITY

Irish Data Protection Commission.

ANNEX II

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

As set out in the MPA.

ANNEX III

LIST OF SUB-PROCESSORS

As set out in the Order.