For more information, or assistance in signing a DPA, please reach out to PrivacyOffice@global.ntt

Data Processing Agreement

Name of party 1	${NTT_Entity_Corporate_Name}	**NTT**
Physical address	${NTT_Entity_PhysicalAddress}	
Postal address	${NTT_Entity_PostalAddress}	
Phone number	${NTT_Entity_TelephoneNumber}	
Email address	${NTT_Entity_EmailAddress}	
Signature (who warrant that they are duly authorized to sign)	_____ For and on behalf of NTT	
Name of signatory		
Title of signatory		
Date of signature		

Name of party 2	${Client_Name}	**Client**
Physical address	${Client_PhysicalAddress}	
Postal address	${Client_PostalAddress}	
Phone number	${Client_TelephoneNumber}	
Email address	${Client_EmailAddress}	
Signature (who warrant that they are duly authorized to sign)	_____ For and on behalf of Client	
Name of signatory		
Title of signatory		
Date of signature		

Supervisory Authority	${Supervisory Authority_Name} If not stated above, the default supervisory authority will be the supervisory authority of the country where the Client's registered office is located, and will be determined by reference to the list of supervisory authorities of the EFTA EEA States found here: https://edpb.europa.eu/about-edpb/about-edpb/members_en

© NTT Ltd. Version 3.1_EU

By signing above, each party acknowledges that it has carefully read and fully understood this data processing agreement and agrees to be bound by the terms of this data processing agreement. If an electronic signature has been used to sign this data processing agreement (whatever form the electronic signature takes) each party agrees that this method of signature is as conclusive of their intention to be bound by this data processing agreement as if signed by each party's manuscript signature.

Contents

1 Introduction

1.1 NTT Ltd. is a leading global technology services company. NTT [insert name of NTT entity] ('**NTT**') is a subsidiary of NTT Ltd. that provides ICT services ('**Services**') to Client under [insert name of relevant agreement OR the existing service agreement] agreement ('**Client Agreement**').

1.2 To the extent NTT may be required to process personal data on behalf of Client under the Client Agreement, NTT will do so in accordance with the terms set out in this Data Processing Agreement ('**DPA**').

2 Defined terms

2.1 '**EC Decision 2021**' means European Commission Decision (EU) 2021/914.

2.2 '**EU SCCs**' means the European Commission's standard contractual clauses for the transfer of personal data from the European Union to third countries as set out in the Annex to the EC Decision 2021, Module Two as set out in Part 1, **Attachment F** and Module Four as set out in Part 2, **Attachment F**.

2.3 '**GDPR**' means the General Data Protection Regulation ((EU) 2016/679).

2.4 '**Restricted Transfer'** means a transfer of personal data from a member state of the European Economic Area ('**EEA**'), the UK or Switzerland (a country not in the EEA or the EU) to a country outside the European Union, EEA, the UK or Switzerland.

2.5 '**Standard Contractual Clauses**' or '**SCCs**' means the EU SCCs and UK SCCs as may be updated, supplemented or replaced from time to time under applicable Data Protection Laws, as a recognized transfer or processing mechanism (as applicable).

2.6 '**UK GDPR**' means the GDPR as implemented in the UK.

2.7 **'UK GDPR Terms**' means those terms otherwise required pursuant to UK GDPR which are not comprised in the SCCs, as set out in **Attachment E**.

2.8 '**UK SCCs**' means the SCCs described in Article 46(2)(c) of the GDPR and approved by the EU Commission Decision 2010/87/EU of 5 February 2010 in **Attachment D**.

2.9 **Lower case terms**. The following lower case terms used but not defined in this DPA, such as '**controller**', '**data subject'**, '**personal data**', '**processor**' and '**processing**' will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether the GDPR applies.

3 Applicable law

3.1 NTT may be required to process personal data on behalf of Client under (a) any applicable law including (b) subordinate legislation and regulations implementing the GDPR and (c) UK GDPR, (collectively referred to '**applicable Data Protection Laws**').

3.2 Unless expressly stated otherwise, in the event of any conflict between (a) the main body of this DPA; and either: (b) the SCCs, or (c) UK GDPR Terms (to the extent the applicable UK GDPR law relating to such terms applies), the applicable local law in (b) will prevail.

3.3 To the extent NTT is a processor of personal data subject to the GDPR and/or UK GDPR, the mandatory sections required by Article 28(3) of the GDPR (or UK GDPR, as applicable) for contracts between controllers and processors that govern the processing of personal data are set out in clauses 5.1, 6.1, 6.3, 6.4, 7, 8.1, 8.2, 9.1, 9.2, 10 to 14 (inclusive). The UK GDPR Terms will govern any processing in relation to any terms required by the UK GDPR which are not covered elsewhere in this DPA.

4 Duration and termination

4.1 This DPA will commence on the date it is signed by the party who signs it last and will remain in force so long as the Client Agreement remains in effect or NTT retains any personal data related to the Client Agreement in its possession or control.

4.2 NTT will process personal data until the date of expiration or termination of the Client Agreement, unless instructed otherwise by Client in writing, or until such personal data is returned or destroyed on the written instructions of Client or to the extent that NTT is required to retain such personal data to comply with applicable laws.

5 Personal data types and processing purposes

5.1 Where the applicable Data Protection Law is the GDPR or UK GDPR:

(a) Client and NTT acknowledge that Client is the controller and NTT is the processor or sub-processor.

(b) The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in **Attachment B**.

5.2 The Client retains control of the personal data and remains responsible for its compliance obligations under applicable Data Protection Laws, including providing any required notices, obtaining any required consents, and for the processing instructions it gives to NTT.

5.3 **Attachment B** describes the purpose of processing and the categories of data subjects and personal data that NTT may process in relation to the Services described in the Client Agreement ('**Business Purposes**').

6 NTT obligations

6.1 **Client instructions**. When NTT acts as the processor of personal data, it will only process the personal data on Client's documented instructions from the categories of persons that the Client authorizes to give personal data processing instructions to NTT, as identified in **Attachment B** ('**Authorized Persons**') and to the extent that this is required to fulfil the Business Purposes. NTT will not process the personal data for any other purpose or in a way that does not comply with this DPA or applicable Data Protection Laws. Should NTT reasonably believe that a specific processing activity beyond the scope of Client's instructions is required to comply with a legal obligation to which NTT is subject, NTT must inform Client of that legal obligation and seek explicit authorization from Client before undertaking such processing. NTT will not process the personal data in a manner inconsistent with Client's documented instructions.

6.2 **Independent controller**. To the extent NTT uses or otherwise processes personal data in connection with NTT's legitimate business operations, NTT will be an independent controller for such use and will be responsible for complying with all applicable laws and controller obligations.

6.3 **Compliance**. NTT will reasonably assist Client in complying with Client's obligations under applicable Data Protection Laws, taking into account the nature of NTT's processing and the information made available to NTT, including in relation to data subject rights, data protection impact assessments and reporting to and consulting with data protection authorities under applicable Data Protection Laws. NTT will immediately notify Client if, in its opinion, any instruction infringes applicable Data Protection Laws. This notification will not constitute a general obligation on the part of NTT to monitor or interpret the laws applicable to Client, and this notification will not constitute legal advice to Client.

6.4 **Disclosure**. NTT will not disclose personal data except: (a) as Client directs in writing, (b) as described in this DPA or (c) as required by law. Where NTT is permitted by law to do so, upon receiving a request from a public authority, NTT will use reasonable endeavors to notify the Client and attempt to redirect the public authority to request the personal data directly from Client.

7 Contracting with sub-processors

7.1 **List of sub-processors**. A list of NTT's sub-processors that NTT directly engages for the specific Services as a processor is available on request from the NTT contact mentioned in **Attachment A,** or as set out in Attachment B, or as otherwise made available on an NTT website.

7.2 **General authorization.** Client provides its general authorization to NTT's engagement with sub-processors, including current and future subsidiaries of NTT Ltd., to provide some or all Services and process personal data on its behalf. To the fullest extent permissible under applicable Data Protection Laws this DPA will constitute Client's general written authorization to the subcontracting by NTT of the processing of personal data to this agreed list of sub-processors.

7.1 **Changes.** NTT will notify the Client in writing of any intended changes to the agreed list of sub-processors at least 14 days in advance, thereby giving the Client the opportunity to object to such changes. Such objection must be made in writing to the NTT contact mentioned in **Attachment A** within 10 days of notification.

7.2 **Performance**. NTT is responsible for its sub-processors' compliance with NTT's obligations in this DPA.

8 Client obligations

8.1 **Data subject requests**. If NTT receives a request from Client's data subject to exercise one or more of its rights under applicable Data Protection Laws, in connection with a Service for which NTT is a processor or sub-processor, NTT will redirect the data subject to make its request directly to Client. Client will be responsible for responding to any such request. NTT will comply with reasonable requests by Client to assist with Client's response to such a data subject request. Client will be responsible for reasonable costs NTT incurs in providing this assistance.

8.2 **Client requests**. NTT must promptly comply with any Client request or instruction from Authorized Persons requiring (a) NTT to amend, transfer, delete or otherwise process the personal data, or to stop, mitigate or remedy any unauthorized processing, (b) Client's obligations regarding security of processing and (c) Client's prior consultation obligations in terms of applicable Data Protection Laws, considering the nature of the processing and the information available to NTT.

8.3 **Warranty**. Client warrants that: (a) it has all necessary rights to provide the personal data to NTT for the processing to be performed in relation to the Services; and (b) NTT's expected use of the personal data for the Business Purposes and as specifically instructed by the Client will comply with all applicable Data Protection Laws.

8.4 **Privacy notices**. To the extent required by applicable Data Protection Laws, Client is responsible for ensuring that all necessary privacy notices are provided to data subjects, and unless another legal basis set forth in applicable Data Protection Laws supports the lawfulness of the processing, that any necessary data subject consents to the processing are obtained and a record of such consents is maintained. Should such a consent be revoked by a data subject, Client is responsible for communicating the fact of such revocation to NTT, and NTT remains responsible for implementing Client's instruction with respect to the processing of that personal data.

9 Security

9.1 **TOMs**. NTT will implement appropriate Technical and Organizational Measures ('**TOMs**') to ensure the security of the personal data in terms of applicable Data Protection Laws, including the security measures set out in **Attachment C**. This includes protecting the personal data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the personal data.

9.2 **Access to personal data.** NTT will grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the Client Agreement. NTT will ensure that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

9.3 **Cost negotiations**. The parties will negotiate in good faith the cost, if any, to implement material changes other than to the extent required by specific updated security requirements set forth in applicable Data Protection Laws or by data protection authorities of competent jurisdiction (in which case NTT would bear the responsibilities of such cost to the extent required by applicable Data Protection Laws or by the data protection authority).

10 Audits

10.1 **Certifications**. NTT will maintain any certifications that it is contractually obligated to maintain and comply with as expressly stated in the Client Agreement. NTT will re-certify against those certifications as reasonably required.

10.2 **Provision of evidence**. At Client's written request, NTT will provide Client with evidence of those certifications relating to the processing of personal data, including applicable certifications or audit reports of its computing environment and physical data centers that it uses in processing personal data to provide the Services, so that Client can reasonably verify NTT's compliance with its obligations under this DPA.

10.3 **Compliance with TOMS**. NTT may also rely on those certifications to demonstrate compliance with the requirements set out in clause 9.1.

10.4 **Confidential information**. Any evidence provided by NTT is confidential information and is subject to non-disclosure and distribution limitations of NTT and/or any NTT sub-processor.

10.5 **Client Audits**. Client may carry out audits of NTT´s premises and operations as these relate to the personal data of Client if:

(a) NTT has not provided sufficient evidence of the measures taken under clause 9; or

(b) an audit is formally required by a data protection authority of competent jurisdiction; or

(c) applicable Data Protection Laws provide Client with a direct audit right (and as long as Client only conducts an audit once in any twelve-month period, unless mandatory applicable Data Protection Laws requires more frequent audits).

NTT Ltd. and its subsidiaries are intended third-party beneficiaries of this section.

10.6 **Client audit process**. The Client audit may be carried out by a third party (but must not be a competitor of NTT or not suitably qualified or independent) who must first enter into a confidentiality agreement with NTT. Client must provide at least 60 days advance notice of any audit unless mandatory applicable Data Protection Laws or a data protection authority of competent jurisdiction requires shorter notice. NTT will cooperate with such audits carried out and will grant Client´s auditors reasonable access to any premises and devices involved with the processing of the Client's personal data. The Client audits will be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. The Client must bear the costs of any Client audit unless the audit reveals a material breach by NTT of this DPA in which case NTT will bear the costs of the audit. If the audit determines that NTT has breached its obligations under the DPA, NTT will promptly remedy the breach at its own cost.

11 Incident management

11.1 **Security incidents**. If NTT becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data while processed by NTT (each a '**Security Incident**'), NTT will promptly and without undue delay:

(a) notify Client of the Security Incident;

(b) investigate the Security Incident and provide Client with sufficient information about the Security Incident, including whether the Security Incident involves personal data of the Client;

(c) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

11.2 **Security incident notification**. Notification(s) of Security Incidents will take place in accordance with clause 11.4. Where the Security Incident involves personal data of the Client, NTT will make reasonable efforts to enable Client to perform a thorough investigation into the Security Incident, to formulate a correct response, and to take suitable further steps in respect of the Security Incident. NTT will make reasonable efforts to assist Client in fulfilling Client's obligation under applicable Data Protection Laws to notify the relevant data protection authority and data subjects about such Security Incident. NTT's notification of or response to a Security Incident under this clause is not an acknowledgement by NTT of any fault or liability with respect to the Security Incident.

11.3 **Other incidents**. NTT will notify Client promptly if NTT becomes aware of:

(a) a complaint or a request with respect to the exercise of a data subject's rights under any applicable Data Protection Laws in relation to personal data NTT processes on behalf of Client and its data subjects; or

(b) an investigation into or seizure of the personal data of Client by government officials, or a specific indication that such an investigation or seizure is imminent; or

(c) where, in the opinion of NTT, implementing an instruction received from Client in relation to the processing of personal data would violate applicable laws to which Client or NTT are subject.

11.4 **Client notifications.** Any notifications made to Client pursuant to this clause 11 will be addressed to the Client contact mentioned in Attachment A using one of the contact methods set out in Attachment A.

12 General cross border transfers of personal data

12.1 Subject to the other provisions of this clause 12 and clause 13, personal data that NTT processes on Client's behalf may be transferred to and stored and processed in any country in which NTT or its sub-processors may operate.

12.2 **Transfer restrictions**. If an applicable Data Protection Law restricts cross-border transfers of personal data, the Client will only transfer that personal data to NTT if NTT, either through its location or participation in a valid cross-border transfer mechanism under the applicable Data Protection Laws, may legally receive that personal data.

12.3 **Change of statutory transfer mechanism**. To the extent that NTT is relying on the SCCs or another specific statutory mechanisms to normalize international data transfers and those mechanisms are subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, Client and NTT agree to cooperate in good faith to promptly suspend the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

13 GDPR and UK GDPR cross border transfers of personal data

13.1 Where the GDPR or UK GDPR is the applicable Data Protection Law, NTT may only process, or permit the processing, of personal data by the Services in respect of a Restricted Transfer under the following conditions:

(a) **Adequacy decision**. Where the European Commission or the UK (as applicable) has found that that the relevant countries provides adequate protection for the privacy rights of data subjects;

(b) **Adequate safeguards**. In the absence of an adequacy decision, where appropriate safeguards have been provided by the controller or processor established in third countries which do not ensure an adequate level of data protection, and who receive the personal data by way of a valid transfer mechanism under Article 46(2) of the GDPR, UK GDPR or other applicable Data Protection Law.

13.1.2 **Standard Contractual Clauses**. SCCs may be used as follows:

(i) the UK SCCs' for personal data subject to UK GDPR , or any successor thereof, including if the UK adopts an addendum to the EU SCCs;

(ii) Module 2 of the EU SCCs for personal data subject to GDPR and/or Swiss Federal Act of 19 June 1992 on Data Protection (**FADP**).

13.2 **Execution of SCCs**. If any cross-border transfer of personal data between NTT and the Client requires execution of SCCs, or execution of successors or addenda to the SCCs mentioned in clause 13.1.2, to comply with the applicable Data Protection Law, the parties will complete all relevant details in, and execute, the applicable SCCs or addenda, and take all other actions required to legitimize the transfer.

13.3 **Sub-processors**. Client authorizes NTT to enter into the applicable form of the applicable SCCs with sub-processors in Client's name and on its behalf (in which case Client will no longer require to enter into direct agreements itself with such sub-processors). NTT will make the executed applicable SCC available to Client on request.

14 Return or destruction of personal data

14.1 **Client deletion.** For certain Services the Client is responsible for installing, hosting, processing and using personal data. Here only Client has the ability to access, extract and delete personal data stored in that Service. Where the particular Service does not support access, retention or extraction of software provided by Client, NTT has no liability for the deletion of personal data as described in this clause 14.1.

14.2 **Delete or return**. Where the Client Agreement requires NTT to retain personal data, NTT will delete that personal data within the time period agreed to in the Client Agreement, unless NTT is permitted or required by applicable law to retain such personal data. Where the retention of personal data has not been addressed in the Client Agreement, NTT will either delete, destroy or return all personal data to Client and destroy or return any existing copies when NTT has finished providing Services:

(a) related to the processing;

(b) this DPA terminates;

(c) Client requests NTT to do so in writing; or

(d) NTT has otherwise fulfilled all purposes agreed in the context of the Services related to the processing activities where Client does not require NTT to do any further processing.

14.3 **Certificate of destruction**. NTT will provide Client with a destruction certificate at Client's request. Where the deletion or return of the personal data is impossible for any reason, or where backups and/or archived copies have been made of the personal data, NTT will retain such personal data in compliance with applicable Data Protection Laws.

14.4 **Third parties**. On termination of this DPA, NTT will notify all sub-processors supporting its own processing and make sure that they either destroy the personal data or return the personal data to Client, at the discretion of Client.

15 Liability and warranty

15.1 Any limitation of liability in the Client Agreement **will apply** to this DPA, other than to the extent such limitation (a) limits the liability of the parties to data subjects or (b) is not permitted by applicable law.

16 Notice

16.1 Any notice or other communication given to a party under or in connection with this DPA must be in writing and delivered to the other party by email.

16.2 Clause 16.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

16.3 Any notice or other communication will be deemed given when:

(a) delivered in person;

(b) received by mail (postage prepaid, registered or certified mail, return receipt requested); or

(c) received by an internationally recognized courier service (proof of delivery received by the noticing party) at the physical notice address (as identified above), with an electronic copy sent to the electronic notice address (as identified in the table above).

17 Miscellaneous

17.1 **Conflict of terms**. The Client Agreement terms remain in full force and effect except as modified in this DPA. Insofar as NTT will be processing personal data subject to applicable Data Protection Laws on behalf of the Client in the course of the performance of the Client Agreement, the terms of this DPA will apply. If the terms of this DPA conflict with the terms of the Client Agreement, the terms of this DPA will take precedence over the terms of the Client Agreement.

17.2 **Governing law**. This DPA is governed by the laws of the country specified in the relevant provisions of the Client Agreement.

17.3 **Dispute resolution**. Any disputes arising from or in connection with this DPA will be brought exclusively before the competent court of the jurisdiction specified in the relevant provisions of the Client Agreement.

17.4 **Counterparts**: This DPA and any SCCs may be executed in any number of counterparts, each of which will constitute an original, but which will together constitute one agreement. Where one or both of the parties choses to execute this DPA and SCCs by electronic signature, each electronic signature will have the same validity and legal effect as the use of a signature affixed by hand and is made with the intention of authenticating this DPA and SCCs and evidencing the intention of that party to be bound by this DPA and SCCs.

© NTT Ltd. Version 3.1_EU

Attachment A Contact points

Contact information of the [data protection officer/compliance officer] of Client:

Contact information: Physical address; phone; email

Contact information of the data protection officer of NTT:

Contact information: Data Protection Officer, PrivacyOffice@global.ntt

© NTT Ltd. Version 3.1_EU

Attachment B Particulars of Processing

1. Categories of data subjects whose personal data is transferred

Data subjects include the Client's representatives, employees, contractors, and customers. NTT acknowledges that, depending on Client's use of the Services, NTT may process the personal data of any of the following types of data subjects:

- Employees, contractors, temporary workers, agents and representatives of data exporter;
- Users (e.g., Client's end users) and other data subjects that are users of Client's Services;
- Juristic persons (where applicable).

2. Categories of personal data transferred

NTT acknowledges that, depending on Client's use of the Services, NTT may process the following types of personal data :

- Basic personal data (for example first name, last name, email address);
- Authentication data (for example username and password);
- Contact information (for example work email and phone number);
- Unique identification numbers and signatures (for example IP addresses);
- Location data (for example, geo-location network data);
- Device identification (for example IMEI-number and MAC address);
- Any other personal data identified in Article 4 of the GDPR.

3. 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.

Biometric Information (for example fingerprints at NTT data centers) [Remove if not applicable to service];

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

Personal data may be transferred on a continuous basis in order to provide the Services under the existing Client Agreement

5. Nature of the processing

The nature of processing personal data is for NTT to provide the Services under the existing Client Agreement. This includes:

- Provision of Services: to provide products and services in line with the governing contract;
- Ticket Resolution: To communicate and co-ordinate resolution of support requests in a timely manner;
- Business Process Improvements: To improve the way services are delivered to our clients;
- Reporting on Contract Performance: To report on contracted services and resolution activities;
- Billing and contract management: to manage contracts, contract renewals and associated invoicing;
- Security and Authentication: To identify and verify the identity of individuals prior to providing access to systems and data; coordinate responses to potential information security events; and
- Administration of systems: To ensure the availability and security of systems.

6. Purpose(s) of the data transfer and further processing

The purpose of processing personal data is for NTT to provide the Services under the existing Client Agreement.

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

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

In accordance with the DPA, NTT may engage sub-processors to provide some or all of the Services on NTT's behalf or use any current or future subsidiaries of NTT Ltd. for the duration of the Client Agreement. Any such sub-processors will be permitted to obtain personal data only to provide some or all of the Services NTT has engaged them to provide, and they are prohibited from using personal data for any other purpose. The list of current NTT Ltd affiliates is attached hereto.

© NTT Ltd. Version 3.1_EU

Attachment C Technical and Organizational Measures

Attachment C describes the Technical and Organizational Measures ('**TOMs**') that NTT maintains to ensure it processes and protects personal data in a responsible way, considering the types of personal data that NTT processes, industry standards, the interests and rights of NTT's employees, clients and communities, and the reasonable cost of implementation in accordance with clause 10 of the DPA and/or as incorporated in Appendix 2 of the applicable SCCs and/or applicable Data Protection Laws.

The NTT TOMs can be found at the following URL:

https://services.global.ntt/en-us/legal/data-privacy-and-protection

At the time of this DPA being signed, the TOMs version in use was: V1.0, last updated 05 Jan 2021

© NTT Ltd. Version 3.1_EU

Attachment D UK Standard Contractual Clauses (processors) – Transfers from the UK

For the purposes of **UK GDPR** for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Please refer to Client details on front page

Tel.: Please refer to Client details on front page; fax: N/A; e-mail: Please refer to Client details on front page

(the data exporter)

And

Name of the data importing organisation: Please refer to NTT details on front page

Address: Please refer to NTT details on front page

Tel.: Please refer to NTT details on front page; fax:N/A ; e-mail: Please refer to NTT details on front page

Other information needed to identify the organisation:

……
(the data importer)

each a “party”; together “the parties”,

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

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'Commissioner'* shall have the same meaning as in the UK GDPR;

(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 covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;

(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 UK;

(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 Commissioner and does not violate the applicable data protection law;

(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 covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of Data Protection Act 2018;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner 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 Commissioner 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 Commissioner;

(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 Commissioner;
   (b) to refer the dispute to the UK courts.
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 Commissioner if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the Commissioner 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 English law.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 of Data Protection Act 2018; or (ii) 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 English law.

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 Commissioner.

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 Commissioner, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Clause 13

Counterparts and electronic signatures

1 These Clauses may be executed in any number of counterparts, each of which will constitute an original, but which will together constitute one agreement.

2 Where one or both of the parties choses to execute these Clauses by electronic signature, each electronic signature will have the same validity and legal effect as the use of a signature affixed by hand and is made with the intention of authenticating these Clauses and evidencing the intention of that party (for itself and for the other data exporters on whose behalf that party is executing these Clauses) to be bound by these Clauses.

© NTT Ltd. Version 3.1_EU

Appendix 1 to the UK Standard Contractual Clauses

Data exporter: **Client** is the data exporter. The data exporter receives Services under the Client Agreement.

Data importer: The data importer is **NTT** and the sub-processors referred to in Attachment B who are involved in the processing of personal data for the Service.

Subject matter: The subject-matter of the processing is limited to personal data within the scope of the section 'Nature and purpose of data processing' (below) and the UK GDPR.

Duration and object of processing. The duration of processing will be for the duration of the Client Agreement between data exporter and NTT. The objective of the data processing is the performance of the Services.

Nature and Purpose of Data Processing. The nature and purpose of processing personal data is for data importer to provide the Services under the existing Client Agreement.

The data importer operates a global network of data centers and support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors operate such facilities.

Data Exporter's Instructions. For all Services, data importer will only act upon data exporter's instructions as conveyed to it.

personal data Deletion or Return. Upon expiration or termination of the Services, data exporter may extract personal data and data importer will delete personal data, each in accordance with the DPA.

Categories of data subjects: See Attachment B.

Categories of personal data: See Attachment B.

Sub-processors: See Attachment B.

Authorized persons: See Attachment B

Appendix 2 to the UK Standard Contractual Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. **Personnel**. Data importer's personnel will not process personal data without authorization.
2. **Data Privacy Contact**. The data privacy officer of the data importer can be reached at the following address:

   NTT

   Attn: Data Protection Officer

   PrivacyOffice@global.ntt

3. **Technical and Organization Measures**. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect personal data, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

The technical and organizational measures, internal controls, and information security routines set forth in Attachment C are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Signing the Standard Contractual Clauses, Appendix 1 and Appendix 2 on behalf of the data importer:

Data Exporter: Please refer to Client details on front page

Signature:

Name:

Designation:

Address:

Data Importer: Please refer to NTT details on front page

Signature:

Name:

Designation:

Address:

Attachment E UK GDPR Terms

To the extent that the DPA does not address all of the issues in this Attachment E or provides lesser data protection commitments to Client in the DPA where NTT processes personal data within the scope of the UK GDPR on behalf of Client, NTT makes the commitments in this Attachment to the Client ('**UK GDPR Terms**', for short). These UK GDPR Terms do not limit or reduce any data protection commitments NTT makes to Client in the Client Agreement.

For purposes of these UK GDPR Terms, Client and NTT agree that Client is the controller and NTT is the processor of personal data, except when Client acts as a processor, in which case NTT is a sub-processor. These UK GDPR Terms do not apply where NTT is a controller of personal data.

1 Supplementary contractual measures

1.1 To the extent that the processing of personal data carried out by NTT is subject to the UK GDPR and NTT makes a transfer to its sub-processor as 'data importer' the obligations set out in 1.1 to 1.11. inclusive will apply.

1.2 Each party warrants that it has no reason to believe that applicable laws to which it is subject, including any requirements to disclose personal data or measures authorising access by public authorities, prevent it from fulfilling its obligations under this DPA and the UK SCCs. Each party declares that in providing this warranty, it has taken due account in particular of the following elements:

(a) the specific circumstances of the processing, including the scale and regularity of processing subject to such applicable laws; the transmission channels used; the nature of the relevant personal data; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by it for the type of personal data processed by it;

(b) the applicable laws to which it is/are subject, including those requiring to disclose data to public authorities or authorising access by such authorities, as well as the applicable limitations and safeguards; and

(c) safeguards in addition to those under this DPA, including the technical and organisational measures applied to the processing of the personal data by NTT and the relevant sub-processor.

1.3 Each party warrants that, in carrying out the assessment under clause 1.2, it has made best efforts to provide Client with relevant information and agrees that it will continue to cooperate with Client in ensuring compliance with this DPA. NTT agrees to document this assessment and make it available to Client on request and it agrees that such assessment may also be made available to a data protection authority.

1.4 NTT agrees to promptly notify Client if, after having agreed to this DPA and for the duration of the term of this DPA, it has reason to believe that it (or a relevant sub-processor to whom a transfer is made) is or has become subject to applicable laws not in line with the requirements under 1.2, including following a change of applicable laws to which is it (or the relevant sub-processor) is subject or a measure (such as a disclosure request) indicating an application of such applicable laws in practice that is not in line with the requirements under clause 1.2. Following such notification, or if Client otherwise has reason to believe that NTT can no longer fulfil its obligations under this DPA (including in relation to the relevant sub-processor), Client (and the relevant subsidiaries who are controllers) will promptly identify appropriate measures (such as, for instance, technical or organisational measures to ensure security and confidentiality) to be adopted by itself or NTT (and/or the relevant sub-processor), at Client's cost, to address the situation, if appropriate in consultation with the competent data protection authority.

1.5 NTT agrees to promptly notify Client if it (or the relevant sub-processor to whom a transfer is made):

(a) receives a legally binding request by a public authority under applicable laws to which it (or the relevant sub-processor) is subject for disclosure of personal data; such notification will include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided;

(b) becomes aware of any direct access by public authorities to personal data in accordance with applicable laws to which it (or the relevant sub-processor) is subject; such notification will include all information available to NTT (and the relevant sub-processor).

1.6 If NTT (or the relevant sub-processor to whom the transfer is made) is prohibited from notifying Client as set out in clause 1.4 it agrees to use its best efforts to obtain (and to procure that the relevant sub-processor obtains) a waiver of the prohibition, with a view to communicate as much information and as soon as possible. NTT agrees to document its (and the relevant sub-processor's) best efforts in order to be able to demonstrate them upon request of Client.

1.7 To the extent permissible under the applicable laws to which NTT (and the relevant sub-processor) is subject, NTT agrees to provide to Client, for the duration of the processing, the relevant information on the requests received by it and the relevant sub-processor (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.).

1.8 NTT agrees to preserve the information pursuant to clauses 1.1 to 1.7 for the duration of the processing and make it available to the competent data protection authority upon request.

1.9 NTT agrees to review (and to procure that the relevant sub-processor to whom the transfer is made will review), having regard to applicable laws to which it (and the relevant sub-processor) is subject, the legality of the request for disclosure, notably whether it remains within the powers granted to the requesting public authority, and to exhaust all available remedies to challenge the request if, after a careful assessment, it (or the relevant sub-processor) concludes that there are grounds under applicable laws to which it (or the relevant sub-processor) is subject to do so. When challenging a request, NTT will (and will procure that the relevant sub-processor will) seek interim measures with a view to suspend the effects of the request until the court has decided on the merits. NTT will not (and will procure that the relevant sub-processor will not) disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are notwithstanding the obligations on NTT pursuant to clause 1.4. NTT agrees to document its (and the relevant sub-processor's) legal assessment as well as any challenge to the request for disclosure and, to the extent permissible under applicable laws to which it (or the relevant sub-processor) is subject, make it available to Client. It will also make it available to the competent data protection authority upon request.

1.10 NTT will use reasonable endeavours to provide (and to procure that the relevant sub-processor to whom the transfer is made will provide) the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

1.11 NTT will inform (and will procure that the relevant sub-processor to whom the transfer is made will inform) data subjects in a transparent and easily accessible format, on its website, of a contact point authorised to handle complaints or requests and NTT will (and will procure that the sub-processors will) promptly deal with any complaints.

EU Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679

(Module 2 – EU Controller to Non-EU Processor transfers)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

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[2] (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;

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

(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) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 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[3]. 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.

---

[3] This requirement may be satisfied by the sub-processor acceding to these clauses under the appropriate Module, in accordance with Clause 7.

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 established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(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

[4] As regards the impact of such laws and practices on compliance with these clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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 governing law as set out in the applicable Client Agreement between the Parties unless otherwise specified.

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 the Member State specified in the Client Agreement between the Parties.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Clause 19

Additional clause relevant to data exporters who are subject to data protection laws in Switzerland

This Clause 19 applies to personal data subject to Switzerland's Federal Act on Data Protection of 19 June 1992 itself and as revised on 25 September 2020 ("FADP"). The term EU Member State in these Clauses includes the EEA States and Switzerland. The data transfer is subject to the provisions of the GDPR. The provisions of the FADP are additionally applicable on a secondary basis. With regard to data transfers of personal data from Switzerland, the Federal Data Protection and Information Commissioner is the competent supervisory authority. Pursuant to the current Federal Act on Data Protection of 19 June 1992 (current as at the date on which these Clauses are entered into) and until the Federal Act on Data Protection of 19 June 1992 as revised on 25 September 2020 enters into force (on or after the date on which these Clauses are entered into), the term personal data with respect to Switzerland includes, in addition, the data of legal entities and not only of natural persons.

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): Client

Name: See Client details on front page.

Address: See Client details on front page.

Contact person's name, position and contact details: See Client details on front page.

Activities relevant to the data transferred under these Clauses: See details of Client Agreement and Description of Transfer.

Signature and date: See Client details on front page.

Role (controller/processor): Controller.

Data importer(s): NTT and the sub-processors referred to in Attachment B who are involved in the processing of personal data for the Service.

Name: See NTT details on front page, as well as the name and details of each of the NTT Group Companies involved in the processing of personal data for the Service referred to in Attachment B.

Address: See NTT details on front page, as well as the address of each of the NTT Group Companies involved in the processing of personal data for the Service referred to in Attachment B.

Contact person's name, position and contact details: See NTT details on front page.

Activities relevant to the data transferred under these Clauses: See details of Client Agreement and Description of Transfer.
Signature and date: See NTT details on front page.

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Attachment B.

Categories of personal data transferred

See Attachment B.

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.

See Attachment B.

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

See Attachment B.

Nature of the processing

See Attachment B.

Purpose(s) of the data transfer and further processing

See Attachment B.

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

See Attachment B.

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

See Attachment B.

C. COMPETENT SUPERVISORY AUTHORITY

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

The competent supervisory authority/ies will be as set out beneath the Client details on the front page of this document.

ANNEX II

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

See Attachment C.