Data Processing Agreement

Name of party 1	${NTT_Entity_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		

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.

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] 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**') as required by the parties and under the relevant data protection laws.

2 Defined terms

2.1 '**Client Data**' means all data, including all text, sound, video or image files, and software, that are provided to NTT by, or on behalf of, Client through use of the Services. Personal data is a category of Client Data.

2.2 **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 any subordinate legislation and regulations implementing the General Data Protection Regulation ((EU) 2016/679) now known as 'EU-GDPR' '**GDPR**'), and any applicable laws, regulations, and other legal requirements relating to (a) data protection and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any personal data in the jurisdictions in which the parties operate. For the avoidance of doubt, this includes 'UK-GDPR' implemented under UK law following the UK's exit from the EU on 31 December 2020. ('**applicable Data Protection Laws**').

4 Duration and termination

4.1 This DPA will commence on the date it is signed by the party who signs it last.

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 data is returned or destroyed on the written instructions of Client.

5 Personal data types and processing purposes

5.1 Client and NTT acknowledge that for the purpose of applicable Data Protection Laws, Client is the controller and NTT is the processor.

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, Appendix 1** describes the purpose of processing and the categories of data subjects and personal data that NTT may process to fulfil the Services described in the Client Agreement or any other purpose specifically identified in **Attachment B, Appendix 1** ('**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, Appendix 1** ('**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. To the extent NTT uses or otherwise processes personal data subject to the GDPR or other applicable Data Protection Laws in connection with NTT's legitimate business operations, NTT will be an independent data controller for such use and will be responsible for complying with all applicable laws and controller obligations. 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 never process the personal data in a manner inconsistent with Client's documented instructions.

6.2 **Purpose pursuit**. The parties have entered into the Client Agreement in order to benefit from the capabilities of NTT in securing and processing the personal data for the purposes set out in **Attachment B, Appendix 1**. NTT will only process personal data per the Client's written instructions.

6.3 **Compliance**. NTT will reasonably assist Client with meeting Client's compliance 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: (1) as Client directs in writing; (2) as described in this DPA; or (3) as required by law. NTT will not disclose personal data to law enforcement agencies unless required by law. If a law enforcement agency contacts NTT with a demand for personal data, NTT will attempt to redirect the law enforcement agency to request that data directly from Client. If compelled to disclose personal data to law enforcement agency, a court, regulator or data protection authority, NTT will promptly notify Client and provide a copy of the demand and give the Client an opportunity to object or challenge the requirement, unless the law prohibits such notice. Upon receipt of any other third-party request for personal data, NTT will promptly notify Client unless prohibited by law. NTT will reject the request unless required by law to comply. If the request is valid, NTT will attempt to redirect the third party to request the data directly from Client.

6.5 **Records of processing activities**. To the extent applicable Data Protection Laws require NTT to collect and maintain records of certain information relating to Client, Client will, where requested, supply such information to NTT and keep it accurate and up to date. NTT may make any such information available to a data protection authority if required by applicable Data Protection Laws. NTT will also keep records regarding the processing of personal data it carries out for the Client relating to, the access, control and security of the personal data, approved sub-contractors, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organizational security measures referred to in section 10.1.

7 NTT employees

7.1 NTT requires that all employees:

(a) undertake training on the applicable Data Protection Laws relating to handling personal data and how it applies to their particular duties; and

(b) are aware both of NTT's duties and their personal duties and obligations under applicable Data Protection Laws.

8 Contracting with sub-processors

8.1 **Sub-processors.** NTT may hire third parties including any subcontractor to provide some or all services and process personal data on its behalf. Client consents to the engagement of these third parties and all current and future subsidiaries and affiliates of NTT Ltd as sub-processors. The above authorizations will constitute Client's prior written consent to the subcontracting by NTT of the processing of personal data to such sub-processors if such consent is required under the Standard Contractual Clauses or applicable Data Protection Laws.

8.2 **List of sub-processors**. A list of NTT Ltd.'s sub-processors is available on request from the NTT contact mentioned in **Attachment A**. NTT may engage new sub-processors from time to time. Where it does so, it will give Clients notice of any new sub-processor at least 14 days in advance of providing that sub-processor with access to personal data. The notice will be given to the Client contact mentioned in **Attachment A**. If Client does not approve a new sub-processor it must send NTT a written objection notice within 14 days of receiving the notice,

setting forth a reasonable basis for objection, where after the parties will make a good-faith effort to resolve the Client's objection. In the absence of a resolution, NTT will make commercially reasonable efforts to provide Client with the same level of service described in the Client Agreement, without using the sub-processor to process Client's personal data. If NTT's efforts are not successful within a reasonable time, but not less than six months, the matter will be determined in accordance with the dispute resolution provisions in the Client Agreement.

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

8.4 **Compatible obligations**. When engaging any sub-processor, NTT will ensure via a written contract that the sub-processor may only access and use personal data to deliver the services NTT has retained them to provide and is prohibited from using personal data for any other purpose. NTT will ensure that sub-processors are bound by written contracts that require them to provide at least the level of data protection required of NTT by the DPA. NTT agrees to oversee the sub-processors to ensure that these contractual obligations are met.

8.5 **Audit**. Client may request that NTT audit the sub-processor or provide confirmation that such an audit has occurred to ensure compliance with its obligations imposed by NTT in conformity with this DPA.

9 Client assistance and client obligations

9.1 **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.

9.2 **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;

(c) Client's obligations under applicable Data Protection Laws that are relevant to the data processing described in **Attachment B, Appendix 1**, including notifications to a data protection authority or to data subjects and the process of undertaking a data protection impact assessment; and

(d) Client's prior consultation obligations in terms of applicable Data Protection Laws;

considering the nature of the processing and the information available to NTT.

9.3 **Warranty**. Client warrants that it has all necessary rights to provide the personal data to NTT for the processing to be performed in relation to the Services, and that one or more lawful bases set forth in applicable Data Protection Laws supports the lawfulness of the processing.

9.4 **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.

10 Security

10.1 **TOMs**. NTT will implement appropriate Technical and Organizational Measures ('**TOMs**') to ensure that the level of security is appropriate to the risks to the personal data in terms of applicable Data Protection Laws, taking into account the:

(a) state of the art (being the most recent level of development of technology of security measures at that particular time);

(b) implementation costs;

(c) processing nature, scope, context and purposes; and

(d) varying risks to data subject's rights and freedoms in terms of likelihood and severity.

These measures will include the security measures agreed upon between the parties in **Attachment B, Appendix 2** as a minimum.

10.2 **Security policies**. Both Client and NTT will maintain written security policies that are fully implemented and applicable to the processing of personal data.

10.3 **Client responsibilities**. Client is solely responsible for making an independent determination as to whether the TOMs for a Service meets Client's requirements, including any of its security obligations under applicable Data Protection Laws. Client acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its personal data as well as the risks to data subjects), the security practices and policies implemented and maintained by NTT provide a level of security appropriate to the risk with respect to personal data that is processed. Client is responsible for implementing and maintaining privacy protections and security measures for components that Client provides or controls.

11 Improvements to security

11.1 **Ongoing evaluation**. The parties acknowledge that security requirements are constantly changing, and that effective security requires frequent evaluation and regular improvements to the security measures undertaken. NTT will therefore evaluate the security measures as implemented in accordance with section 10 on an on-going basis in order to maintain compliance with the requirements set out in section 10.

11.2 **Cost negotiations**. The parties will negotiate in good faith the cost, if any, to implement material changes required by specific updated security requirements set forth in applicable Data Protection Laws or by data protection authorities of competent jurisdiction.

11.3 **Amendment negotiations**. Where an amendment to the Client Agreement is necessary in order to execute a Client's written instruction to NTT to improve security measures as may be required by changes in applicable Data Protection Laws from time to time, the parties will negotiate an amendment to the Client Agreement in good faith.

12 Audits

12.1 **Certifications**. NTT will maintain any approved certifications recognized under applicable Data Protection Laws that are listed in the Client Agreement between the parties. NTT will recertify those certifications as reasonably required. Prior to processing personal data and at Client's request, NTT will provide Client with copies of any certifications it maintains (along with relevant supporting documentation) that apply to the systems, policies, and procedures that govern the processing of personal data. NTT may rely on certifications to demonstrate compliance with the requirements set out in section 11, provided that the requirements contained in **Attachment B, Appendix 2** are also addressed by such certifications.

12.2 **Client Audits**. Client will be entitled to carry out audits of NTT´s premises and operations as these relate to the personal data if:

(a) NTT has not provided sufficient evidence of the measures taken under section 10.1 as a result of a self-audit or assurance type report;

(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).

12.2.2 **Client audit process**. The 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

and will grant Client´s auditors reasonable access to any premises and devices involved with the processing of the 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.

13 Incident management

13.1 **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 Client 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;

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

Notification(s) of Security Incidents will take place in accordance with section 13.3. Where the Security Incident involves personal data, NTT will make reasonable efforts to enable Client to perform a thorough investigation into the 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 GDPR Article 33 or other 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 section is not an acknowledgement by NTT of any fault or liability with respect to the Security Incident.

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

(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 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.

13.3 **Notifications.** Any notifications made to Client pursuant to this section 13 will be addressed to the Client contact mentioned in **Attachment A** using one of the contact methods set out in **Attachment A**.

14 Data transfers

14.1 **Generally**. Except as described elsewhere in the DPA, 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.

14.2 **Transfer mechanisms**. NTT may only process, or permit the processing, of personal data by the Services from a member state of the European Economic Area ('**EEA**') (including the UK) or Switzerland to a country outside the European Union, EEA and Switzerland under the following conditions:

(a) **Adequacy decision**. Where the European Commission has found that that the countries listed here provides adequate protection for the privacy rights of data subjects: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en;

(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 or other applicable Data Protection Law. NTT will identify in **Attachment B, Appendix 1** the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and the Provider must immediately inform the Customer of any change to that status.

14.3 **Standard Contractual Clauses** ('**SCCs**'). NTT may use the SCCs as described in Article 46(2)(c) of the GDPR and approved by the EU Commission Decision 2010/87/EU of 5 February 2010, or any successor standard contractual clauses that may be adopted pursuant to an EU Commission decision in **Attachment B** as a recognized transfer mechanism. Where SCCs are used, the parties will complete all relevant details in, and execute the SCCs. If Client consents to NTT (located in the EEA) appointing a sub-processor located outside the EEA, then Client authorizes NTT to enter into SCC contained in **Attachment B** with the sub-processor in Client's name and on its behalf. NTT will make the executed SCC available to Client on request.

14.4 **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.

14.5

15 Return or destruction of client data and personal data

15.1 **Client deletion.** For certain Services, the Client is responsible for installing, hosting, processing and using Client Data. Here only Client has the ability to access, extract and delete personal data in the Client 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 section 15.1.

15.2 **Delete or return**. Where the Client Agreement requires NTT to retain Client Data, NTT will delete that Client Data within the time period agreed to in the Client Agreement, unless NTT is permitted or required by applicable law to retain such Client Data. Where the retention of Client Data has not been addressed in the Client Agreement, NTT will, at the discretion of Client, either delete, destroy or return all Client 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.

15.3 **Certificate of destruction**. NTT will provide Client with a destruction certificate at Client's request and follow Client's instructions about what to do with backups and archived copies of the Client Data on deletion, or where return of the Client Data is impossible for any reason.

15.4 **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 Client Data or return the Client Data to Client, at the discretion of Client.

16 Liability

16.1 Any limitation of liability set forth in the Client Agreement **will apply** to this DPA.

17 Notice

17.1 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.

17.2 Section 17.1 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.

17.3 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).

18 Miscellaneous

18.1 **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 with the Client, 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.

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

18.3 **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.

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:
pivacyoffice@global.ntt

Attachment B Standard contractual clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, **Client (as data exporter) and NTT (as data importer)**, whose signature appears below), each a 'party,' together 'the parties,' have agreed on the following Contractual Clauses (the 'Clauses' or 'Standard Contractual Clauses') in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of data subjects for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1: Definitions

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

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

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

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

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

(f) 'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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 below which forms an integral part of the Clauses.

Clause 3: Third-party beneficiary clause

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

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

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

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

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

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

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

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 below;

(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, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

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

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

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

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

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

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

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

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

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

(c) that it has implemented the technical and organizational 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 unauthorized access, and

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

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

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

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

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

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

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

Clause 6: Liability

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

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

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

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

Clause 7: Mediation and jurisdiction

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

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

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

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

Clause 8: Cooperation with supervisory authorities

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

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

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

Clause 9: Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10: Variation of the contract

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

Clause 11: Subprocessing

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

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for

compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

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

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

Clause 12: Obligation after the termination of personal data processing services

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

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

This appendix contains multiple versions of the Services information. One or many may apply depending on the precise Services contained within the applicable order form or agreement.

The information in this appendix is relevant regardless of whether the SCCs are executed

Please note that additional sub-processors may be included dependant on the Service arrangement in place

Appendix 1a to the Standard Contractual Clauses (Support Services)

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

Data importer: The data importer is **NTT**.

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 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. These include:

- 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
- Application and device logs (e.g. call logs, access logs, server logs, etc. as related to the Service provided)
- Business Process Improvements: To improve the way services are delivered.
- 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 Compliance: To identify and verify the identity of individuals prior to providing access to systems and data

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.

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

Categories of data subjects:

- Employees, contractors, temporary workers, agents and representatives of the Controller;
- Users (e.g. clients end users) and other data subjects that are users of the Services;).

Categories of personal data: NTT acknowledges that, depending on Client's use of the Services, the data importer may process the personal data from any of the following categories in the Client Data:

- Basic personal data (e.g. first name, last name, company, job title, business unit or department and business activities);
- Business Contact information (e.g. work email, phone number, video address, etc.);
- User Credentials related to the Services provided;
- Device and Technical Information related to the Service provided (e.g. IP addresses, IMEI-number, MAC address, etc.); and
- Location data (e.g. geo-location network data).

Legal basis for processing personal data outside the EEA in order to comply with cross-border transfer restrictions

- Located in a country with a current determination of adequacy
- Standard Contractual Clauses between Client as 'data exporter' and NTT as 'data importer'
- Standard Contractual Clauses between NTT as 'data exporter' on behalf of Client and NTT affiliate or sub-processor as 'data importer'.

Sub-processors: In accordance with the DPA, the data importer may hire third parties to provide processing services on data importer's behalf or use any of its affiliates. Any such sub-processors will be permitted to obtain personal data only to deliver the services the data importer has retained them to provide, and they are prohibited from using personal data for any other purpose.

Name of Sub Processor	**Delivery Location**	**Legal Entity**	**Registered Address**
NTT Global Delivery Centre (GDC)	India (Bangalore)	NTT India GDC Private Ltd	Milestone Buildcon Pvt. Ltd, No. 32/1, 35, 37-47, Chokkanahalli Village, Off. Thanisandra Main Road, Yelahanka, Banagalore Bangalore, KA 560064, India
NTT Global Delivery Centre (GDC)	Czech Republic (Prague)	NTT Europe GDC s.r.o.	Pikrtova 1737/1a, Prague 140 00, Czech Republic
NTT Global Delivery Centre (GDC)	Malaysia (Kuala Lumpur)	NTT MSC Sdn. Bhd.	No.43000, Persiaran APEC, 63000 Cyberjaya, Selangor, Malaysia

As a global organization, NTT may transfer data to additional office locations in order to facilitate data processing including system hosting, administration and maintenance:

- South Africa
- Australia
- Malaysia
- Within the European Union, including Netherlands, Romania, Ireland and Czech Republic
- United Kingdom

Appendix 1b to the Standard Contractual Clauses (Managed Services)

Data importer: The data importer is **NTT**.

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 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. These include:

- 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.
- 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 Compliance: To identify and verify the identity of individuals prior to providing access to systems and data

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.

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

Categories of data subjects:

- Employees, contractors, temporary workers, agents and representatives of the Controller;
- Users (e.g. clients end users) and other data subjects that are users of the Services;).

Categories of personal data: NTT acknowledges that, depending on Client's use of the Services, the data Basic personal data (e.g. first name, last name, company, job title, business unit or department and business activities);

- Business Contact information (e.g. work email, phone number, video address, etc.);
- User Credentials related to the Services provided
- Application and device logs (e.g. call logs, access logs, server logs, etc.)
- Device and Technical Information related to the Service provided (e.g. IP addresses, IMEI-number, MAC address, etc.);
- Location data (e.g. geo-location network data);

Legal basis for processing personal data outside the EEA in order to comply with cross-border transfer restrictions

- Located in a country with a current determination of adequacy
- Standard Contractual Clauses between Client as 'data exporter' and NTT as 'data importer'

- Standard Contractual Clauses between NTT as 'data exporter' on behalf of Client and NTT affiliate or sub-processor as 'data importer'.

Sub-processors: In accordance with the DPA, the data importer may hire third parties to provide processing services on data importer's behalf or use any of its affiliates. Any such sub-processors will be permitted to obtain personal data only to deliver the services the data importer has retained them to provide, and they are prohibited from using personal data for any other purpose.

Name of Sub Processor	**Delivery Location**	**Legal Entity**	**Registered Address**
NTT Global Delivery Centre (GDC)	India (Bangalore)	NTT India GDC Private Ltd	Milestone Buildcon Pvt. Ltd, No. 32/1, 35, 37-47, Chokkanahalli Village, Off. Thanisandra Main Road, Yelahanka, Banagalore Bangalore, KA 560064, India
NTT Global Delivery Centre (GDC)	Czech Republic (Prague)	NTT Europe GDC s.r.o.	Pikrtova 1737/1a, Prague 140 00, Czech Republic
NTT Global Delivery Centre (GDC)	Malaysia (Kuala Lumpur)	NTT MSC Sdn. Bhd.	No.43000, Persiaran APEC, 63000 Cyberjaya, Selangor, Malaysia
Managed Hybrid Infrastructure Services (MHIS CoE)*	Spain (Barcelona)	NTT Managed Services EMEA, S.A.U	Av. Diagonal 575, ed. L'Illa, modulo II, planta 9 08029 Barcelona
Managed Network Services (MNS CoE)	India (Bangalore)	NTT India GDC Private Ltd	Milestone Buildcon Pvt. Ltd, No. 32/1, 35, 37-47, Chokkanahalli Village, Off. Thanisandra Main Road, Yelahanka, Banagalore Bangalore, KA 560064, India
Managed Collaboration Services (MCS CoE)	South Africa (Port Elizabeth)	NTT Ltd Management Services South Africa (Pty) Ltd	2nd Floor Wanderers Building, The Campus, 57 Sloane Street, Bryanston, GP, 2021, South Africa
Group Delivery Centre (Secure24)	• US (various) • India (Hyderabad) • Germany • Netherlands • Switzerland	NTT Managed Services India Private Limited	Western Dallas, 12'th floor, Hitech city Hyderabad, Telangana, 500081
Managed Service Centre (MSC)	Frankfurt	NTT Germany Holdings GmbH	Horexstraße 7, 61352 Bad Homburg, German
Managed Service Centre (MSC)	United Kingdom	NTT Germany Holdings GmbH	Horexstraße 7, 61352 Bad Homburg, German
Managed Service Centre (MSC)	Prague	NTT Germany Holdings GmbH	Horexstraße 7, 61352 Bad Homburg, German
EU MIM Centre	Bangalore	NTT India GDC Private Ltd	North Wing 11-13, BCIT, Milestone Buildcon SEZ, Chokkanahalli Village, Off. Thanisandra Main Road, Yelahanka, Bangalore 560064, Karnataka, India

As a global organization, NTT may transfer data to additional office locations in order to facilitate data processing including system hosting, administration and maintenance:

- South Africa
- Australia
- Malaysia
- Within the European Union, including Netherlands, Romania, Ireland and Czech Republic
- United Kingdom

Appendix 2 to the 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: 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:

A description of the technical and organizational measures, is available on the NTT website (https://hello.global.ntt/en-us/legal/data-privacy-and-protection) which 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: [Name of Client]

Signature:

Name:

Designation:

Address:

Data Importer: [Name of NTT Entity]

Signature:

Name:

Designation:

Address: