Data Processing Agreement

Contents

1 Introduction

1.1 This Data Processing Agreement ('**DPA**') forms part of the agreement between NTT DATA and Supplier ('**Supplier Agreement**') under which Supplier agrees to provide NTT DATA or a NTT DATA Affiliate with certain solutions, products and/or services ('**Solutions**').

1.2 To the extent Supplier may be required to process personal data on behalf of NTT DATA or a NTT DATA Affiliate under the Supplier Agreement, Supplier will do so under the terms set out in this DPA.

2 Defined terms

2.1 '**Affiliate**' means a legal entity that controls, is controlled by or that is under common control with either NTT DATA or Supplier. For the purposes of this definition, control' means the power to direct the management and policies of an entity through voting rights, contract or otherwise. For purposes of NTT DATA, this includes NTT DATA, Inc. and all its direct and indirect subsidiaries

2.2 '**Additional Safeguards**' means those terms set out in section 6 of Attachment D.

2.3 '**CCPA**' means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199).

2.4 '**China or PRC**' means the People's Republic of China, excluding for the purposes of this DPA, Hong Kong SAR, Macau SAR and Taiwan.

2.5 '**China Data Protection Laws**' means the Cybersecurity Law of the PRC, Data Security Law of the PRC, Personal Information Protection Law of the PRC and other laws, regulations, administrative rules and compulsory national standards of the PRC.

2.6 '**Customer**' means the entity to whom NTT DATA or a NTT DATA Affiliate provides services, and '**Regulated Customer**' means any Customer that is subject to mandatory sector-specific regulatory, supervisory or statutory requirements imposed by a governmental, regulatory or supervisory authority, including requirements relating to operational resilience, information and communication technology, cybersecurity, data protection, safety, reliability, or continuity of services.

2.7 '**Customer Agreement**' means the agreement between Customer or Regulated Customer and NTT DATA or NTT DATA Affiliate.

2.8 '**Data Exporter**' means a party that is transferring Personal Data directly or via onward transfer to a country that triggers additional requirements for the protection of Personal Data being transferred under the applicable Data Protection Laws.

2.9 '**Data Importer**' means a party that receives Personal Data directly from a Data Exporter, or via onward transfer, and that is located in a country that triggers additional requirements for the protection of Personal Data being transferred under the applicable Data Protection Laws.

2.10 '**Data Protection Laws**' means any mandatory laws applicable to a party in connection with the processing of personal data under the Supplier Agreement including but not limited to (each as amended or replaced from time to time) (a) EU Data Protection Laws, (b) UK Data Protection Laws, (c) the CCPA, (d) the Swiss Federal Act of 19 June 1992 on Data Protection and the Swiss Federal Act on Data Protection of 25 September 2020, as revised or replaced from time to time ('**FADP**'), (e) China Data Protection Laws, (f) the Indian Digital Personal Data Protection Act, 2023, (g) Brazilian General Data Protection Law, Law No. 13,709/2018 ("**LGPD**"), and the applicable regulations and transfer mechanisms issued by Brazil's National Data Protection Authority ("**ANPD**") (h) Turkish Personal Data Protection Law No. 6698 and (g) any applicable laws worldwide relevant to Supplier, NTT DATA or Customers (where applicable and as recipients of services provided by NTT DATA) relating to data protection cross-border transfers, outsourcing notifications, approvals or registrations, data localization, or equivalent transfer mechanisms.

2.11 '**EU**' means the European Union.

2.12 '**EU Data Protection Laws**' means the GDPR, any successor thereto, and any other law relating to the data protection or privacy of individuals that applies in the European Economic Area.

2.13 '**EU SCCs**' means Sections I, II, III and IV (as applicable) in so far as they relate to Module Two (Controller-to-Processor), Module Three (Processor-to-Processor) and Module Four (Processor-to-Controller), as applicable, within the Standard Contractual Clauses for the transfer of Personal Data to third countries under Regulation (EU) 2016/679 of the European Parliament and the Council approved by EC Commission Decision of 4 June 2021, as set out in **Attachment D**.

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

2.15 '**Personal Data**' means all personal data provided to Supplier by, or on behalf of, NTT DATA, including data generated, derived or collected through the use of the Solutions.

2.16 '**Restricted Transfer**' means a transfer of Personal Data from a Data Exporter to a Data Importer.

2.17 '**Standard Contractual Clauses**' or '**SCCs**' means any pre-approved jurisdiction-specific standard contractual clauses or equivalent approved transfer terms required under applicable Data Protection Laws and any substantially equivalent standard contract or regulator-approved transfer terms that may become applicable in for the international transfer of personal data under applicable Data Protection Laws, including the EU SCCs, the Swiss Addendum UK Addendum, Brazilian SCCs, and Turkish standard contracts 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).

2.18 '**Standard Contract**' or '**China SCCs**' means the **Standard Contract For Personal Information Exports** for the transfer of Personal Data from a Data Exporter in China to a Data Importer located outside of China issued by the Cyberspace Administration of China ('**CAC**') or alternative standard contract clauses as may be approved by the CAC from time to time. En English translation of the Standard Contract is available here.

2.19 '**sub-processor**'' means any processor engaged by Supplier that processes Personal Data pursuant to the Supplier Agreement.

2.20 '**Swiss Addendum**' means the EU SCCs as amended by **Attachment E**.

2.21 '**UK**' means the United Kingdom of Great Britain and Northern Ireland.

2.22 '**UK Addendum**' means the template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament under s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the Mandatory Clauses of the Addendum. The UK Addendum is set out in **Attachment E**.

2.23 '**UK Data Protection Laws**' means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

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

2.25 **Lower case terms**. The following lower-case terms used but not defined in this DPA, such as '**controller**', '**data subject**', '**personal data**', '**personal data breach**', '**processor**' and '**processing**' will have the same meaning as set forth in Article 4 of the GDPR, or where not specifically defined under Data Protection Laws, the same meaning as analogous terms in those Data Protection Laws.

3 Legal relationships

3.1 NTT DATA and Supplier acknowledge that for purposes of this DPA,:

(a) NTT DATA is the controller of Personal Data and Supplier its processor, or

(b) Customer is the controller of Personal Data, NTT DATA its processor and Supplier NTT DATA's sub-processor.

4 Applicable law

4.1 Supplier may be required to process Personal Data on behalf of NTT DATA under applicable Data Protection Laws.

4.2 Unless expressly stated otherwise, in the event of any conflict between (a) the main body of this DPA; and Data Protection Laws, applicable Data Protection Law will prevail.

4.3 If Supplier is processing personal data within the scope of specific jurisdictions that are not contained in the main body of this DPA, such terms shall be contained in Attachments to this DPA. The additional terms do not limit or reduce any data protection commitments Supplier makes to NTT DATA in the DPA, Supplier Agreement or other agreement between Supplier and NTT DATA. Where Personal Data originates from a jurisdiction not expressly listed in this DPA, nor in an Attachment that imposes processor-specific obligations or cross-border transfer requirements, Supplier shall comply with such requirements and provide protections no less protective than those set out in this DPA. Without limiting the foregoing, where Supplier processes Personal Data within the scope of the CCPA, the California Consumer Privacy Act Terms set out in **Attachment F** will apply to such processing.

4.4 Where the Solutions involve biometric data, telecommunications traffic data, communications content data, or other categories of data subject to sector-specific laws, Supplier shall comply with the applicable sector-specific requirements, including any confidentiality, notice, consent, retention and deletion requirements applicable to the Solutions and Supplier's role.

5 Duration and termination

5.1 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 Supplier Agreement remains in effect or Supplier retains any Personal Data related to the Supplier Agreement in its possession or control.

5.2 Supplier will process Personal Data until the date of expiration or termination of the Supplier Agreement, unless instructed otherwise by NTT DATA in writing, or until such Personal Data is returned or destroyed on the written instructions of NTT DATA or to the extent that Supplier is required to retain such Personal Data to comply with applicable laws.

6 Personal data types and processing purposes

6.1 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 concerning the Solutions described in the Supplier Agreement ('**Business Purposes**'), are specified in **Attachment B**.

6.2 NTT DATA 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 Supplier.

7 Supplier obligations

7.1 **NTT DATA instructions**. Supplier warrants that it will only process the Personal Data on NTT DATA's documented instructions from the categories of persons that NTT DATA authorizes to give Personal Data processing instructions to Supplier, as identified in **Attachment B** ('**Authorized Persons**') and to the extent that this is required to fulfil the Business Purposes. Supplier warrants that it 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. Supplier further warrants that it will not process Personal Data or perform its obligations under this DPA in such a way as to cause NTT DATA or any NTT DATA Affiliate to be in breach of applicable Data Protection Laws. Should Supplier reasonably believe that a specific processing activity beyond the scope of NTT DATA's instructions is required to comply with a legal obligation to which Supplier is subject, Supplier must inform NTT DATA of that legal obligation and seek explicit authorization from NTT DATA before undertaking such processing. Supplier will not process the Personal Data in a manner inconsistent with NTT DATA's documented instructions. Supplier will immediately notify NTT DATA if, in its opinion, any instruction from NTT DATA infringes applicable Data Protection Laws.

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

7.3 **Use restrictions.** For the avoidance of doubt, unless expressly authorized in writing by NTT DATA, Supplier shall not: (a) sell, share or otherwise disclose Personal Data for targeted advertising or other unrelated commercial purposes; or (b) use Personal Data, or permit Personal Data to be used, to develop, train, fine-tune, evaluate, calibrate, or otherwise improve any artificial intelligence, foundation model or other machine learning model.

7.4 **Disclosure**. Supplier warrants that it will not disclose Personal Data except: (a) as NTT DATA directs in writing, (b) as described in this DPA or (c) as required by law. If a public authority contacts Supplier with a demand for Personal Data, Supplier must redirect the public authority to request the Personal Data directly from NTT DATA. If compelled to disclose Personal Data to a public authority, Supplier will promptly notify NTT DATA and provide a copy of the demand and allow NTT DATA to object or challenge the demand, unless the law prohibits such notice. Upon receipt of any other third-party request for Personal Data, Supplier will promptly notify NTT DATA unless prohibited by law. Supplier will reject the request unless required by law to comply. If the request is valid, Supplier will redirect the third party to request the Personal Data directly from NTT DATA.

7.5 **Records of processing activities**. Supplier will keep detailed, accurate and up-to-date written records regarding the processing of Personal Data it carries out for NTT DATA including, but not limited to, the access, control and security of the Personal Data, approved sub-processors, 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. Supplier will ensure that the records are sufficient to enable NTT DATA to verify Supplier's compliance with its obligations under this DPA and Supplier will provide NTT DATA with copies of the records upon request.

7.6 **Collection of Personal Data**: Where the parties agree in writing that Supplier is required to collect Personal Data on behalf of NTT DATA, Supplier will only collect Personal Data for NTT DATA using a notice or method that NTT DATA specifically pre-approves in writing, which contains an approved data privacy notice informing the data subject of NTT DATA's identity, the purpose or purposes for which Personal Data will be processed, and any other information that, having regard to the specific circumstances of the collection and expected processing, is required to enable fair processing. Supplier will not modify or alter the notice in any way without NTT DATA's prior written consent.

7.7 **Assistance**: Supplier will provide the following assistance to NTT DATA at Supplier's cost:

(a) promptly notify NTT DATA of any request it has received from NTT DATA or Customer's data subject and redirect the data subject to make the request directly to NTT DATA. The Supplier must not respond to the request itself unless authorized to do so by NTT DATA;

(b) promptly comply with any NTT DATA request or instruction from Authorized Persons requiring Supplier to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorized processing;

(c) assist NTT DATA in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations, Supplier must comply with NTT DATA's instructions;

(d) assist NTT DATA in ensuring compliance with the following obligations, considering the nature of the data processing and the information available to the Supplier:

(i) the obligation to assess the impact of the envisaged processing operations on the protection of Personal Data where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(ii) the obligation to consult the competent data protection authorities before processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken to mitigate the risk;

(iii) the obligation to ensure that Personal Data is accurate and up to date, by informing NTT DATA without delay if Supplier becomes aware that the Personal Data it is processing is inaccurate or has become outdated; and

(iv) obligations regarding notification of a data breach to a data protection authority or data subject under applicable Data Protection Laws.

7.8 **Regulated Customers**: In addition, where relevant to the Solutions, Supplier will provide reasonable information and cooperation necessary for NTT DATA or its Affiliates or Regulated Customers to comply with mandatory requirements relating to operational resilience, information and communication technology, cybersecurity, data protection, safety, reliability, continuity of services, subcontracting oversight, third-party risk management disaster recovery, incident response, testing, cooperation with competent authorities and regulators, and the orderly return, deletion, transition or exit of Personal Data.

8 Contracting with sub-processors

8.1 **Specific prior authorization.** Supplier may hire any subcontractor ('**sub-processor'**) to provide some or all Solutions and process Personal Data on its behalf but Supplier may only authorize a sub-processor to process the Personal Data if:

(a) NTT DATA has provided its specific written authorization to do so;

(b) Supplier has submitted a notice to NTT DATA requesting specific authorization before the engagement of the sub-processor, together with full details regarding such sub-processor and any other information necessary to enable NTT DATA to decide on the authorisation;

(c) NTT DATA is provided with an opportunity to approve or object to the appointment of each sub-processor under clause 8.2 below;

(d) Supplier enters into a written contract with the sub-processor that imposes in substance the same data protection obligations on them as the ones imposed on the Supplier by this DPA (in particular, about requiring appropriate technical and organizational data security measures), and, upon NTT DATA's written request, provide NTT DATA with copies of such contracts and any subsequent amendments; and

(e) Supplier remains responsible for all Personal Data it entrusts to the sub-processor.

8.2 **Notification.** The notice containing the request for specific authorization of the engagement of a sub-processor will be given to the NTT DATA contact mentioned in **Attachment A**. If NTT DATA does not approve a new sub-processor it must send Supplier a written objection notice within 10 days of receiving the notice, setting forth the objection, where after the parties will make a good-faith effort to resolve NTT DATA's objection. In the absence of a resolution, Supplier will make commercially reasonable efforts to provide NTT DATA with the same level of service described in the Supplier Agreement, without using the sub-processor to process NTT DATA's Personal Data. If Supplier's efforts are not successful within a reasonable time, the matter will be determined under the dispute resolution provisions in the Supplier Agreement.

8.3 **Agreed list of sub-processors**. A list of Supplier's sub-processors that Supplier engages for the Solutions as a processor is set out in **Attachment B** (as applicable). Any changes to the sub-processors will require NTT DATA's specific prior authorization in terms of clause 8.2.

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

8.5 **Compatible obligations**. When engaging any sub-processor, Supplier will ensure via a written contract that the sub-processor may only access and use personal data to deliver the services Supplier has retained them to provide and is prohibited from using Personal Data for any other purpose. Supplier will oversee the sub-processors to ensure that these contractual obligations are met.

8.6 **Audit**. NTT DATA may request that Supplier audit the sub-processor or confirm that such an audit has occurred or a copy of the audit results where NTT DATA requests them to do so, to ensure Supplier's compliance with its obligations imposed by Supplier in conformity with this DPA.

9 Security

9.1 **TOMs**. Supplier 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.** Supplier 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 the Supplier Agreement. Supplier 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 **Supplier personnel.** Supplier must ensure that all members of its personnel:(a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data; (b) undertake training on the applicable Data Protection Laws relating to handling Personal Data and how it applies to their particular duties; and (c) are aware both of Supplier's duties and their duties and obligations under applicable Data Protection Laws.

9.4 **Security policies**. Supplier will maintain written security policies that are fully implemented and applied to the processing of Personal Data. At a minimum, these policies must include assignment of internal responsibility for information security management, devoting adequate personnel resources to information security, carrying out appropriate background checks on permanent staff who will have access to the Personal Data, requiring employees, vendors and others with access to Personal Data to enter into written confidentiality agreements, and conducting training to make employees and others with access to the Personal Data aware of information security risks presented by the processing.

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

10 Audits

10.1 **Certifications**. Supplier will maintain any certifications that it is contractually obligated to maintain and comply with as expressly stated in the Supplier Agreement, or approved certifications recognized under applicable Data Protection Laws. Supplier will re-certify against those certifications as reasonably required.

10.2 **Supplier self-audits**. At least once a year, Supplier will conduct site audits of its personal data processing practices and the information technology and information security controls for all facilities (including physical data centers that it uses to process NTT DATA Personal Data) so that NTT DATA can reasonably verify Supplier's compliance with its obligations under this DPA. The audit must include obtaining a network-level vulnerability assessment. Each audit must be performed by well-recognized, qualified, independent, third-party security auditors based on recognised industry best practices, at Supplier's selection and expense. Each audit will result in the generation of an audit report ('**Supplier Audit Report**'). As required by any Supplier Agreement and if NTT DATA requests it, Supplier will provide NTT DATA with the relevant Supplier Audit Report. NTT DATA must treat the Supplier Audit Reports as Supplier's confidential information under the Supplier Agreement. The Supplier Audit Report will be subject to non-disclosure and distribution limitations of Supplier and the auditor. Supplier will promptly address any issues noted in the Supplier Audit Reports with the development and implementation of a corrective action plan to the satisfaction of the auditor as soon as possible but not longer than one month.

10.3 **NTT DATA Audits**. NTT DATA may carry out audits of Supplier´s premises and operations as these relate to the Personal Data of NTT DATA if:

(a) Supplier 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 NTT DATA with a direct audit right (and as long as NTT DATA only conducts an audit once in any twelve months, unless mandatory applicable Data Protection Laws require more frequent audits).

Supplier must bear the costs of any NTT DATA audit carried out under clauses 10.3(a) and 10.3(b) as well as where the audit reveals a material breach by Supplier of this DPA.

10.4 **NTT DATA audit process**. NTT DATA may choose to carry out the audit itself or mandate an independent third-party auditor (but must not be a competitor of Supplier or not suitably qualified or independent) who must first enter into a confidentiality agreement with Supplier. NTT DATA 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. Supplier will cooperate with such audits carried out and will grant NTT DATA´s auditors reasonable access to any premises and devices involved with the processing of NTT DATA's Personal Data. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. NTT DATA must bear the costs of any NTT DATA audit unless the audit is carried out under clauses 10.3(a) and 10.3(b) or the audit reveals a material breach by Supplier of this DPA in which case Supplier will bear the costs of the audit. If the audit determines that Supplier has breached its obligations under the DPA, Supplier will promptly remedy the breach at its own cost.

11 Incident management

11.1 **Security Incidents**. If Supplier 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 Supplier (each a '**Security Incident**'), Supplier will promptly, and in any event within 24 hours:

(a) notify NTT DATA of the Security Incident;

(b) investigate the Security Incident and provide NTT DATA with sufficient information about the Security Incident, including whether the Security Incident involves Personal Data of NTT DATA;

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

11.2 **Security Incident Notification**. Notification(s) of Security Incidents will take place under with clause 11.4. Where the Security Incident involves Personal Data of NTT DATA, Supplier will make reasonable efforts to enable NTT DATA 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. Supplier will make reasonable efforts to assist NTT DATA in fulfilling NTT DATA's obligation under applicable Data Protection Laws to notify the relevant data protection authority and data subjects about such Security Incident.

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

(a) a complaint or a request concerning the exercise of a data subject's rights under any applicable Data Protection Laws about Personal Data Supplier processes on behalf of NTT DATA and its data subjects; or

(b) an investigation into or seizure of the Personal Data of NTT DATA by government officials, or a specific indication that such an investigation or seizure is imminent; or

(c) where, in the opinion of Supplier, implementing an instruction received from NTT DATA about the processing of Personal Data would violate applicable laws to which NTT DATA or Supplier are subject.

11.4 **Notifications.** Any notifications made to NTT DATA under this clause 11 will be addressed to the NTT DATA contact mentioned in **Attachment A** using one of the contact methods set out in **Attachment A**. The notifications should contain:

(a) a description of the nature of the Security Incident, including where possible the categories and approximate number of data subjects concerned, and the categories and approximate number of Personal Data records concerned;

(b) the name and contact details of Supplier's data protection officer or another contact point where more information can be obtained;

(c) a description of the likely consequences of the Security Incident;

(d) a description of the measures taken or proposed to be taken by Supplier to address the Security Incident including, where appropriate, measures to mitigate its possible adverse effects.

11.5 **Co-operation**. Immediately following any Security Incident, the parties will co-ordinate with each other to investigate the matter. Supplier will reasonably co-operate with NTT DATA in NTT DATA's handling of the matter, including:

(a) assisting with any investigation;

(b) providing NTT DATA with access to any facilities and operations affected;

(c) facilitating interviews with Supplier's employees, former employees and others involved in the matter;

(d) making available all relevant records, logs, files, data reporting and other materials required to comply with all applicable Data Protection Laws or as otherwise reasonably required by NTT DATA; and

(e) taking reasonable and prompt steps to mitigate the effects and minimise any damage resulting from the incident.

11.6 **Notifications to third parties**. The Supplier will not inform any third party of the Security Incident without first obtaining NTT DATA's prior written consent, except when required to do so by law. Supplier agrees that NTT DATA has the sole right to determine:

(a) whether to provide notice of the Security Incident to any data subjects, data protection authorities, law enforcement agencies or others, as required by law or in NTT DATA's discretion, including the contents and delivery method of the notice; and

(b) whether to offer any type of remedy to affected data subjects, including the nature and extent of such remedy.

11.7 **Other Supplier obligations**. To the extent that the following is not specifically addressed in the Supplier Agreement, Supplier will:

(a) cover all reasonable expenses associated with the performance of its obligations above unless the matter arose from NTT DATA's specific instructions, negligence, wilful default or breach of this DPA, in which case NTT DATA will cover all reasonable expenses;

(b) restore Personal Data at its own expense; and

(c) reimburse NTT DATA for actual reasonable expenses that NTT DATA incurs when responding to a Security Incident to the extent that the Supplier caused the Security Incident, including all costs of notice and any remedy.

12 Cross border transfers of Personal Data

12.1 **General**. Personal Data that Supplier processes on NTT DATA's behalf may not be transferred to and stored and processed in any country in which Supplier or its sub-processors may operate, except as provided for in this clause 12.

12.2 **Restricted Transfers**. Where there is a Restricted Transfer of Personal Data, the Data Exporter and the Data Importer must transfer and process the Personal Data under all applicable Data Protection Laws. In particular:

(a) **Attachment D** will apply where Personal Data that is subject to EU Data Protection Laws is transferred from a Data Exporter to a Data Importer acting as a Processor;

(b) **Attachment E** will apply where Personal Data that is subject to applicable Data Protection Laws in the specific jurisdiction provisions set forth in **Attachment E** is transferred outside the listed jurisdictions.

12.3 **Execution of SCCs**. If any cross-border transfer of Personal Data between Supplier and NTT DATA requires the execution of SCCs to comply with the applicable Data Protection Law, the parties' signature to this DPA or the Supplier Agreement will be considered as signature to the SCCs. Where the SCCs are the EU SCCs, Annex I must be signed in addition to this DPA or Customer Agreement. Such signature must comply with the national law governing the EU SCCs.

12.4 **Change of statutory transfer mechanism**. To the extent that Supplier is relying on the EU SCCs or another specific statutory mechanism to normalize international data transfers and those mechanisms are subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, NTT DATA and Supplier 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 Return or destruction of Personal Data

13.1 **Delete or return**. Where the Supplier Agreement requires Supplier to retain Personal Data, Supplier will delete that Personal Data within the period agreed to in the Supplier Agreement, unless Supplier is permitted or required by applicable law to retain such Personal Data. Where the retention of Personal Data has not been addressed in the Supplier Agreement, Supplier will at its cost either delete, destroy or return all Personal Data to NTT DATA and destroy or return any existing copies when Supplier has finished providing Solutions:

(a) related to the processing;

(b) when this DPA terminates;

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

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

13.2 **Certificate of destruction**. Supplier will provide NTT DATA with a destruction certificate at NTT DATA'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, Supplier will retain such Personal Data in compliance with applicable Data Protection Laws.

13.3 **Third parties**. On termination of this DPA, Supplier will notify all sub-processors supporting its processing and make sure that they either destroy the Personal Data or return the Personal Data to NTT DATA, at the discretion of NTT DATA.

14 Liability and indemnity

14.1 Supplier indemnifies NTT DATA and holds NTT DATA and NTT DATA Affiliates harmless against all claims, actions, third party claims (including by a Customer or any data subject), losses, damages and expenses (including penalties and fines assessed against NTT DATA, legal costs or other costs incurred by NTT DATA in connection with investigating, mitigating, remediating and/or complying with notification (or other mandated regulatory) requirements in connection with a Security Incident) that NTT DATA or any NTT DATA Affiliate incur arising out of a breach of this DPA or applicable Data Protection Laws by Supplier, provided that:

(a) NTT DATA provides Supplier with a notice of the claim promptly after receiving it;

(b) NTT DATA gives Supplier the right to control the defence;

(c) NTT DATA provides the indemnifying party with reasonable assistance as necessary; and

(d) NTT DATA avoids any admission of liability.

14.2 Unless the parties have agreed otherwise in the Supplier Agreement, the indemnity provided by Supplier in this clause 14 will not be limited by any limitation of Supplier's liability and/or exclusions of the Supplier's liability set forth in the Supplier Agreement.

15 Notice

15.1 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.

15.2 Clause 15.1 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.

15.3 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).

16 Miscellaneous

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

16.2 **Governing law**. This DPA is governed by the laws of the country specified in the relevant provisions of the Supplier Agreement and the EU SCCs and UK Addendum are governed by the laws as provided for in the EU SCCs or UK Addendum.

16.3 **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 Supplier Agreement.

16.4 **Counterparts**: This DPA 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 chooses to execute this DPA 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 to authenticate this DPA and evidence the intention of that party to be bound by this DPA.

16.5 **Amendments**. NTT DATA will publish any intended amendments to this DPA on an NTT DATA website or send written notification to the Supplier at least 14 days in advance, allowing the Supplier to object to such amendments. Such objection must be made in writing to the NTT DATA contact mentioned in **Attachment A** within ten days of notification. Supplier's failure to submit a written objection to the intended amendments within ten days of notification, will be deemed acceptance of the amendments to this DPA.

Attachment A Contact points

Contact information of the data protection officer of NTT DATA:

Contact information: Ashleigh Meiring; Executive, Data Privacy & Protection; privacyoffice@global.ntt

Contact information of the data protection officer of Supplier:

Contact information: Where applicable, as set forth in the Supplier Agreement or information about the Supplier's representative under Article 4(17) in conjunction with Article 27 of the GDPR in the EU and UK GDPR, or as provided for on the Supplier's website or to be provided by the Supplier in writing.

Attachment B Particulars of Processing

Categories of data subjects whose personal data is transferred

Supplier acknowledges that, depending on NTT DATA's use of the Solutions, Supplier may process the Personal Data of any of the following types of data subjects:

- Employees, contractors, temporary workers, job applicants, agents and representatives of NTT DATA and Affiliates;
- Users (e.g., Customers' end users);
- Legal persons (where applicable).

Categories of personal data transferred

Supplier acknowledges that, depending on NTT DATA's use of the Solutions, the types of Personal Data processed by Supplier may include, but are not limited to the following:

- Basic personal data (for example first name, last name, email address, home address and work address);
- National insurance/identification number;
- Bank account information;
- Authentication data (for example username and password);
- Contact information (for example work email and phone number);
- Professional or employment-related information (for example, employer name and job title);
- Educational information (for example, educational background or certifications),
- Unique identification numbers and signatures (for example IP addresses);
- Location data (for example, geo-location network data); and
- Device identification (for example IMEI-number and MAC address).

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.

Supplier acknowledges that, depending on NTT DATA's use of the Solutions, Supplier may process sensitive data including:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Records of criminal offenses;
- Data concerning the health of a data subject;
- Data concerning the sex life of a data subject;
- Sexual orientation; and
- Biometric information.

Supplier will notify NTT DATA in writing to the extent Supplier needs to collect additional sensitive data beyond those listed above in order to provide the Solutions. Please see **Attachment C** for applied restrictions.

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

Continuous basis for the duration of the Supplier Agreement.

Nature of the processing

The Personal Data transferred will be subject to the following basic processing activities:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organisation and structuring
- Using data, including analysing, consultation, testing, automated decision making and profiling
- Updating data, including correcting, adaptation, alteration, alignment and combination
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion.

Purpose(s) of the data transfer and further processing

The purpose of processing personal data is for Supplier to provide the Solutions to NTT DATA under the existing Supplier Agreement.

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

See clause 13 of the DPA

Authorized persons. Supplier will only process the personal data on NTT DATA's documented instructions from the following categories of persons that NTT DATA authorizes to give personal data processing instructions to Supplier:

Senior employees within NTT DATA or Affiliates, and as otherwise advised from NTT DATA in writing from time to time

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

The following Supplier sub-processors have been authorized by NTT DATA upon signature of this DPA:

Name	Country	Subject matter and nature of the processing	Duration of the processing

Attachment C Technical and Organizational Measures

Attachment C describes the Technical and Organizational Measures ('**TOMs**') that Supplier maintains to ensure it processes and protects Personal Data in a responsible way, considering the types of Personal Data that Supplier processes, industry standards, the interests and rights of NTT DATA's employees, clients and communities, and the reasonable cost of implementation in accordance with clause 9 of the DPA.

Supplier maintains and enforces the following minimum TOMs as outlined in **Attachment C**.

(A) Data Privacy and Protection Measures

1 Governance and Operating Model

1.1 Supplier is committed to demonstrating accountability when Supplier processes Personal Data and has implemented an organizational structure, and roles and responsibilities for managing and providing oversight over the processing of Personal Data.

1.2 Several governance structures have been implemented to ensure that data privacy and protection matters are reviewed by appropriate senior management of the Supplier. Ultimate accountability for data privacy and protection is held by the highest level of management in Supplier and is supported by designated roles throughout the business, including appointed Data Protection Officers or equivalent roles, where required under applicable Data Protection Laws.

2 Policies, processes and Guidelines

2.1 Supplier has implemented and communicated its policies, processes, standards and guidelines that detail how Supplier employees are expected to process Personal Data.

2.2 Supplier has defined and communicated privacy notices that provide information about how Personal Data is processed.

2.3 Supplier has a Data Protection Impact Assessment ('**DPIA**') process and performs DPIAs when required following applicable Data Protection Laws.

3 Data Protection by Design

3.1 Supplier is committed to implementing reasonable measures to support NTT DATA's ability to comply with applicable Data Protection Laws. As far as possible, the principles of data protection by design and by default are applied during the development and delivery of Supplier products, services and solutions.

3.2 Supplier applies data minimization principles and, to the extent reasonably possible, will limit the Personal Data processed to what is adequate, relevant and necessary for the Business Purposes.

4 Data Landscape

4.1 Supplier has implemented processes to identify, record, assess and maintain an accurate understanding of the Personal Data that Supplier processes.

4.2 Supplier maintains a record of the Personal Data processed in accordance with applicable Data Protection Laws and this DPA.

5 Information Lifecycle Management

5.1 Supplier has implemented policies and processes to ensure that Personal Data is processed appropriately throughout its lifecycle (from collection through to use, retention, disclosure and destruction).

5.2 Applicable Data Protection Laws in certain countries provide data subjects with specific rights in relation to their Personal Data. Supplier is committed to upholding these rights and ensuring that Supplier supports NTT DATA in responding to data subject requests in a transparent, fair, ethical and lawful way.

5.3 Supplier maintains a record of all data subject requests received and the actions taken to respond to these requests. Supplier will provide support to NTT DATA in responding to data subject requests in accordance with the DPA.

5.4 Supplier only retains Personal Data where there is a legitimate business purpose and in accordance with the Supplier agreement and the DPA. Supplier destroys, deletes or de-identifies Personal Data when the retention period lapses and there is no legitimate business reason to retain the Personal Data for a longer period.

5.5 Supplier keeps the Personal Data processed on behalf of NTT DATA in accordance with DPA and will destroy, delete, de-identify or return Personal Data when requested, to NTT DATA, and where there are no further obligations to retain the Personal Data under applicable law.

5.6 Supplier has measures in place to ensure that Personal Data is accurate, complete and up to date.

5.7 Supplier has appropriate mechanisms in place, as outlined in the DPA to support the lawful transfer Personal Data outside of the country where it was originally collected and have appropriate agreements in place with NTT DATA and Supplier subsidiaries, affiliates, and sub-processors to support cross-border transfers.

6 Data Subject Rights

6.1 Data protection laws in certain countries provide data subjects with specific rights about their personal data. Supplier is committed to upholding these rights and ensuring that Supplier responds to data subject requests in a transparent, fair, ethical and lawful way.

6.2 Supplier has implemented appropriate policies to uphold the data subject rights in accordance with applicable data protection laws.

6.3 Supplier supports the following data subject rights:

(a) right to be informed;
(b) right of access;
(c) right to rectification;
(d) right to be forgotten;
(e) right to data portability;
(f) right to restrict use;
(g) right to object (including the right to opt-out of direct marketing and the sale of personal data);
(h) right to challenge automated decisions; and
(i) right to complain.

6.4 Supplier maintains a record of all data subject requests received and the actions taken to respond to these requests.

6.5 Supplier will provide all reasonable support to NTT DATA in responding to data subject requests, where requested, and in accordance with the Supplier Agreement and the DPA.

6.6 Supplier is committed to ensuring that Supplier respond to all requests from public authorities to access Personal Data in accordance with applicable laws, and the terms of the DPA.

7 Cross-border Transfers

7.1 Supplier relies on appropriate statutory mechanisms to normalize international data transfers and has appropriate agreements in place to support cross-border transfers of Personal Data.

7.2 Where Personal Data is transferred across borders, Supplier performs transfer impact assessments to determine whether the country to which Personal Data is transferred offers the same level of protection to the rights and freedoms of data subjects as the original country. Where gaps are identified, Supplier has implemented supplementary measures to support data subject rights in accordance with its policies and ensure that Personal Data is processed in a transparent, fair and ethical way.

8 Regulatory

8.1 Supplier is committed to keeping abreast of changes to data protection laws in the countries in which Supplier operates and has implemented processes to support compliance.

9 Training and Awareness

9.1 Supplier requires all employees to complete data privacy and protection training periodically. All data privacy and protection policies, processes, standards and guidelines are available to employees and communicated regularly.

10 Security for Privacy

10.1 Taking into account the state of the art, cost of implementation and the nature, scope, context and purpose of processing Personal Data, as well as the risks to the rights and freedoms of data subjects; Supplier has implemented appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of Personal Data.

10.2 Without limiting the foregoing, Supplier will maintain risk-appropriate controls for encryption of Personal Data in transit and at rest, multi-factor authentication for remote access and privileged access where technically feasible, and vulnerability and patch management processes commensurate with the risks presented by the Solutions.

11 Breach Response and Notification

11.1 Supplier has policies, processes and procedures for identifying, detecting, responding, recovering and notifying appropriate stakeholders in the event of a Personal Data breach. This includes mechanisms for performing a root cause analysis and undertaking corrective actions.

11.2 Supplier is committed to ensuring that Supplier notifies NTT DATA without undue delay in the event of a Personal Data breach in compliance with applicable Data Protection Laws and the DPA.

11.3 Supplier maintains a record of all Personal Data breaches and the actions taken to respond to these events and may provide this on request to NTT DATA.

12 Third Party Management

12.1 Supplier is accountable for the actions of its processors (i.e. sub-processors) who process Personal Data on Supplier's behalf and assesses the ability of its processors to protect Personal Data at the time of selection and periodically thereafter in accordance with Supplier policies.

12.2 Supplier processors are required to sign appropriate agreements that govern the processing and protection of Personal Data and require the same obligations, as outlined in the DPA, to be transferred to any further processors who Supplier may engage in accordance with the DPA. Supplier has ensured that data processing agreements are in place with all its processors (or sub-processors), that uphold the same standard of care as outlined in the DPA.

(B) Information Security Measures

Supplier is committed to ensuring that information security control is implemented and properly managed to protect the confidentiality, integrity and availability of Personal Data processed on behalf of and under the instruction of NTT DATA.

13 Information Security Roles and Responsibilities

13.1 Roles and responsibilities for information security have been formally assigned, with reporting lines that ensure the independence of the function.

13.2 Supplier employees are responsible for ensuring that they act in accordance with the information security policies, processes, standards and guidelines in their day-to-day business activities.

14 Information Security Policies

14.1 Supplier has documented and published a set of information security policies that are aligned to industry best practices and standards for information security and reviewed periodically. Those policies address the following:

(a) mobile device management;
(b) workplace surveillance;
(c) acceptable use;
(d) asset management and classification;
(e) access controls;
(f) encryption and key management;
(g) network security;
(h) application security;
(i) back ups;
(j) system security;
(k) physical and environmental security;
(l) operational security; and
(m) system acquisition, development and maintenance.

15 Human Resources

15.1 Supplier performs background and employment screening for its employees, to the extent permitted under applicable law, to ensure their suitability for hiring and handling company and NTT DATA information (including Personal Data). The extent of the screening is proportional to the business requirements and classification of information that the employee will have access to.

15.2 Supplier requires that Supplier employees (including contractors and temporary employees) agree to maintain the confidentiality of NTT DATA information and Personal Data.

15.3 Supplier employees are required to complete information security awareness training on an annual basis. Information security policies and supporting procedures, processes and guidelines are made available to employees and employees receive relevant information about trends, threats and best practices.

16 Third Party Management

16.1 Supplier has policies and supporting procedures to ensure that information assets are protected when Supplier engages third party service providers and/or processors (sub-processors). This includes requirements for information security due diligence and information security risk assessments to be performed to ensure:

(a) Information Security requirements are clearly articulated and documented in the agreements with Supplier processors;

(b) Supplier processors implement the same level of protection and control as Supplier;

(c) Processors are required to report any suspected or actual information security incidents to Supplier promptly.

16.2 Supplier has undertaken reasonable efforts to ensure that appropriate written agreements are in place with processors who have access to Personal Data, NTT DATA information, applications, systems, databases and infrastructure. These agreements include information security standards for ensuring the confidentiality, integrity and availability of Personal Data and NTT DATA information.

17 Information Security Incident Management

17.1 Supplier has policies, processes and procedures for identifying, detecting, responding, recovering and notifying appropriate stakeholders in the event of an information security incident, including Personal Data breaches. This includes mechanisms for performing a root cause analysis and undertaking corrective actions.

18 Business Continuity

18.1 Supplier has established business continuity and disaster recovery plans.

19 Compliance with Laws

19.1 Supplier has established roles and responsibilities for identifying laws and regulations that affect Supplier's business operations.

Attachment D EU Standard Contractual Clauses

1 Definitions

1.1 For the purposes of this **Attachment D**, the following definitions will apply:

(a) '**C-to-P Transfer Clauses**' means Sections I, II, III and IV (as applicable) in so far as they relate to Module Two (Controller-to-Processor) within the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by EC Commission Decision of 4 June 2021.

(b) '**P-to-C Transfer Clauses**' means Sections I, II, III and IV (as applicable) in so far as they relate to Module Four (Processor-to-Controller) within the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by EC Commission Decision of 4 June 2021.

(c) '**P-to-P Transfer Clauses**' means Sections I, II, III and IV as applicable) in so far as they relate to Module Three (Processor-to-Processor) within the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by EC Commission Decision of 4 June 2021.

2 All modules

2.1 If, in the performance of the Solutions, Personal Data that is subject to EU Data Protection Laws is transferred from a Data Exporter to a Data Importer, then the parties must comply with the terms of the EU SCCs (as further described in section 3 to 5 below) and the following provisions will apply:

(a) Clause 7 (docking clause) of the EU SCCs will not apply.

(b) The option under Clause 11 (redress) of the EU SCCs will not apply.

(c) Any dispute arising from the EU SCCs will be resolved by the courts of is the Netherlands.

(d) Annex I.A to the EU SCCs (List of the Parties): The activities relevant to the transfer of Personal Data under the EU SCCs relate to the provision/ reception of the Solutions received/provided by NTT DATA/Supplier (see details on front page) under the Supplier Agreement. **Attachment A** includes the contact person's name, position and contact details. The parties agree that their signature to the Supplier Agreement, to this DPA or to any other binding document which otherwise incorporates the DPA will be considered as signature to the SCCs in accordance with the terms set out therein.

(e) The contents of **Attachment B** will form Annex I.B to the EU SCCs (Description of Transfer).

(f) The Dutch Data Protection Authority will act as the competent supervisory authority for the purposes of Annex I.C of the EU SCCs (Competent Supervisory Authority).

3 C-P Transfer Clauses

3.1 Where NTT DATA is the controller and Data Exporter of Personal Data and Supplier is a processor and Data Importer in respect of that Personal Data, then the parties must comply with the terms of the C-to-P Transfer Clauses and the following provisions will also apply:

(a) Option 1 under Clause 9(a) (specific prior authorization) will apply and '[Specify time period]' will be replaced with '30 (thirty) days';

(b) For the purposes of Clause 13(a) (supervision), the Data Exporter will be considered as established in an EU Member State;

(c) Option 1 under Clause 17 (governing law) will apply and the governing law will be the law of the Netherlands.

(d) The contents of **Attachment C** to this DPA (Technical and Organizational Measures) will form Annex II of the C-P Transfer Clauses (Technical and organisational measures including technical and organisational measures to ensure the security of the data); and

(e) The list of sub-processors at **Attachment B** to this DPA will form Annex III of the C-P Transfer Clauses (List of Subprocessors).

4 P-P Transfer Clauses

4.1 Where Customer is the controller of the Personal Data, NTT DATA is the processor acting on behalf of a Customer and Data Exporter and Supplier is a sub-processor and Data Importer of that Personal Data, then the parties will comply with the terms of the P-to-P Transfer Clauses and the following provisions will also apply.

(a) For the purposes of Clause 8.6(c) and (d) (security of processing), Supplier must provide notification of a personal data breach concerning Personal Data processed by Supplier to NTT DATA (only) and not directly to Customer. Where appropriate, NTT DATA will forward the notification to the relevant Customer;

(b) For the purposes of Clause 8.9 (documentation and compliance), all enquiries from Customer will be provided to Supplier by NTT DATA. If Supplier receives an enquiry directly from Customer, it must forward the enquiry to NTT DATA and will not respond to the enquiry without NTT DATA's consent;

(c) Option 2 under Clause 9 (general written authorization) will apply and '[Specify time period]' be replaced with '30 (thirty) days'. The parties also agree that Customer has delegated the decision making and approval authority for sub-processing to NTT DATA for the purposes of Clause 9 (use of sub-processors). Supplier has NTT DATA's general authorization (on behalf of Customer) for the engagement of the sub-processors listed in **Attachment B** to this DPA. Supplier must follow the process set out in clause 8.2 of this DPA to inform NTT DATA (only) and not Customer of any intended changes to that list. Where appropriate, NTT DATA will inform Customer of any changes;

(d) For the purposes of Clause 10 (data subject rights), Supplier must notify NTT DATA (only) and not Customer about any request it has received directly from a data subject. Where appropriate, NTT DATA will forward the notification to the relevant Customer. The authorization to respond to the request must be provided to Supplier by NTT DATA on behalf of Customer. Supplier must assist NTT DATA as well as Customer in fulfilling the relevant obligations to respond to any such request;

(e) For the purposes of Clause 11 (redress), Supplier will only inform data subjects through individual notice in its capacity as the Data Importer where required by applicable Data Protection Laws to which the Data Importer is subject. In such case, Supplier must (to the extent permitted by applicable Data Protection Laws) inform NTT DATA of that legal requirement before Supplier provides the individual notice. It must immediately inform NTT DATA if it receives a complaint by a data subject concerning Personal Data and must not respond to such complaint without first informing, and obtaining permission where appropriate, from NTT DATA;

(f) For the purposes of Clause 13(a) (supervision), the Data Exporter will be considered as established in an EU Member State;

(g) For the purposes of Clause 15 (obligations of the data importer in case of access by public authorities), Supplier must notify NTT DATA (only) and not the data subject(s) in case of access by public authorities. Where appropriate, NTT DATA will notify Customer and/or the affected data subject as necessary. Supplier agrees to provide information on request for access by public authorities to NTT DATA in accordance with section 6 of this Attachment D. In the event Supplier receives a request from the competent data protection authorities for the information it preserves pursuant to Clauses 15.1 (a) to (c) or 15.2(b) under the P-P Transfer Clauses it must inform NTT DATA and involve NTT DATA in responding to the competent data protection authority;

(h) Option 1 under Clause 17 (governing law) will apply and the governing law will be the law of the Netherlands; and

(i) The contents of **Attachment C** to this DPA (Technical and Organizational Measures) will form Annex II of the P-P Transfer Clauses (Technical and organisational measures including technical and organisational measures to ensure the security of the data).

5 P-C Transfer Clauses

5.1 Where Supplier is the processor and Data Exporter of Personal Data and NTT DATA is a controller and Data Importer in respect of that Personal Data, then the parties will comply with the terms of the P-to-C Transfer Clauses and the governing law in Clause 17 (governing law) will be the law the Netherlands.

6 Additional Safeguards to the EU SCCs

6.1 To the extent that the EU SCCs apply and Supplier is acting as Data Importer, Supplier must comply with the additional safeguards to the EU SCCs set out in this section 6 of this **Attachment D**.

6.2 Where in NTT DATA's reasonable opinion transfer impact assessments, or risk assessments, are necessary, the Supplier will upon request promptly provide reasonable assistance and cooperation to NTT DATA (at the Supplier's own cost) about the carrying out of the transfer impact assessments, or risk assessments, in order to enable NTT DATA to normalize the international data transfers.

6.3 Supplier 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 Data Protection Laws. Supplier 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 authorizing 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 Supplier and the relevant sub-processor.

6.4 Supplier warrants that, in carrying out the assessment under section 6.3 above, it has made its best efforts to provide NTT DATA with relevant information and agrees that it will continue to cooperate with NTT DATA in ensuring compliance with this DPA. Supplier agrees to document this assessment and make it available to NTT DATA on request and it agrees that such assessment may also be made available to a data protection authority.

6.5 Supplier agrees to promptly notify NTT DATA if, after having agreed to this DPA and for the duration of the term of this DPA, Supplier 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 section 6.3, 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 section 6.3. Following such notification, or if NTT DATA otherwise has reason to believe that Supplier can no longer fulfil its obligations under this DPA (including in relation to the relevant sub-processor), Supplier (or a relevant sub-processor to whom a transfer is made) will promptly identify supplementary measures (such as, for instance, technical or organisational measures to ensure security and confidentiality) to be adopted by itself (and/or the relevant sub-processor), at Supplier's cost, to protect the Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security, if appropriate in consultation with the competent data protection authority.

6.6 Supplier further warrants that:

(a) it has not purposefully created any means by which a public authority can bypass Supplier's security mechanisms, authentication procedures and/or software to gain access to and/or use its systems and/or the Personal Data received from NTT DATA, such as a back door or similar programming;

(b) it has not purposefully created or changed its business processes, security mechanisms, software and/or authentication procedures in a manner that facilitates access to its systems and/or the Personal Data received from NTT DATA by public authorities; and

(c) it is not required by national law or government policy to create or maintain any means to facilitate access to its systems and/or the Personal Data received from NTT DATA by public authorities, such as back door, or for Supplier to be in possession or to hand over the encryption key to access such data.

6.7 Any audits, including requests for reports or inspections, carried out by NTT DATA or a qualified independent assessor selected by NTT DATA (the '**Independent Assessor**') of the processing activities will include, at the choice of NTT DATA and/or the Independent Assessor, verification as to whether any Personal Data received by NTT DATA has been disclosed to public authorities and, if so, the conditions under which such disclosure has been made.

6.8 Supplier agrees to promptly notify NTT DATA 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. Supplier agrees to review (and to procure that the relevant sub-processor to whom the transfer is made will review) the request, 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. The notification to NTT DATA will include information about the Personal Data requested, the requesting authority and the legal basis for the request;

(b) becomes aware of any direct access by public authorities to Personal Data under applicable laws to which it (or the relevant sub-processor) is subject; such notification will include all information available to Supplier (and the relevant sub-processor).

6.9 If Supplier (or the relevant sub-processor to whom the transfer is made) is prohibited by applicable law from notifying NTT DATA as set out in section 6.8, Supplier agrees 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, Supplier 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 and to communicate as much information and as soon as possible to NTT DATA. Supplier 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. Supplier 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 NTT DATA. It will also make it available to the competent data protection authority upon request.

6.10 Supplier will promptly inform the requesting public authority if, in Supplier's opinion, such request is inconsistent and/or conflicts with its obligations pursuant to the EU SCCs. Supplier will document any such communication with the public authorities relating to the inconsistency and/or conflict of such request with the EU SCCs.

6.11 Supplier 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.

6.12 Supplier will not make any disclosures of the Personal Data received from NTT DATA to any public authority that are determined to be massive, disproportionate and indiscriminate in a manner that it would go beyond what is necessary in a democratic society.

6.13 To the extent permissible under the applicable laws to which Supplier (and the relevant sub-processor) is subject, Supplier agrees to provide on an annual basis to NTT DATA, for the duration of the processing, the relevant information on the requests received by it and the relevant sub-processor. Where possible, such information must include the following:

(a) number and nature of requests;

(b) type of data requested;

(c) requesting authority or authorities;

(d) an overview of the laws and regulations that permit access to the Personal Data in the jurisdiction to which Supplier is subject, to the extent [data importer/Supplier] is reasonably aware of such laws and regulations;

(e) whether requests have been challenged and the outcome of such challenges;

(f) any measures taken to prevent access by public authorities to the Personal Data received from NTT DATA;

(g) the legal basis to disclose the Personal Data received from NTT DATA to the public authority; and

(h) whether Supplier reasonably believes that it is legally prohibited to provide the information in (a) to (g) above and, if so, the extent to which such prohibition applies.

6.14 Supplier agrees to preserve the information under section 6.13 for the duration of the processing and make it available to the competent data protection authority upon request.

6.15 Supplier will comply with internal policies governing the disclosure of Personal Data in response to requests from public authorities.

6.16 Supplier 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 Supplier will (and will procure that the sub-processors will) promptly deal with any complaints about requests from public authorities.

Attachment E Cross-border specific jurisdiction provisions

1 General

1.1 In the interest of meeting their obligations under Data Protection Laws, the parties agree that this General section1 of **Attachment E** will apply where:

(a) Personal Data is transferred from a Data Exporter to a Data Importer; and

(b) the jurisdiction from which the Personal Data originates recognizes the EU SCCs as an adequacy mechanism, or such jurisdiction has not adopted another legally sufficient transfer mechanism under Data Protection Laws or such Restricted Transfer is not otherwise governed by country-specific laws, under this **Attachment E**, or

(c) the cross-border transfer mechanism for the Data Importer to process Personal Data outside China to comply with cross-border transfer restrictions is either a Security Assessment by the CAC, the China SCC's or a Personal Information Protection Certification.

1.2 For the purposes of this General section of **Attachment E**, the EU SCCs will be amended as follows:

(a) the EU SCCs are deemed to be amended to the extent necessary so they operate:

(i) for transfers made by the Data Exporter to the Data Importer, to the extent that applicable Data Protection Laws apply to the Data Exporter's processing when making that Restricted Transfer; and

(ii) to provide appropriate safeguards for the transfers in accordance with applicable Data Protection Laws.

(b) references to 'Regulation (EU) 2016/679' or 'that Regulation' in the EU SCCs must be understood as references to 'applicable Data Protection Laws';

(c) references to specific articles of 'Regulation (EU) 2016/679' in the EU SCCs are removed and replaced with the equivalent article or section of applicable Data Protection Laws, where appropriate;

(d) references to 'Regulation (EU) 2018/1725' are removed;

(e) references to a 'Member State' or 'EU Member States' in the EU SCCs must be understood as references to 'the country where the Data Exporter is established', except for Clause 11(c)(i), where applicable, where reference to 'Member State' will be replaced with 'country'; and

(f) the footnotes to the EU SCCs are removed.

1.3 For the avoidance of any doubt, the parties do not intend to grant third-party beneficiary rights to data subjects under the EU SCCs when those data subjects would not otherwise benefit from such rights under Data Protection Laws. The higher level of protection provided by the EU SCCs will only apply in jurisdictions outside Europe where such a higher level of protection is required for the protection of Personal Data being transferred under Data Protection Laws.

1.4 If applicable Data Protection Laws require a jurisdiction-specific transfer mechanism, filing, approval or registration not expressly addressed in this Attachment E, the parties shall cooperate in good faith to implement such mechanism or another lawful alternative to the extent applicable to the Solutions.

2 China

2.1 Where a Restricted Transfer of Personal Data is required, the Data Importer may only lawfully receive and process Personal Data in a foreign jurisdiction through one of the following cross-border transfer mechanisms available under China Data Protection Law:

(a) a mandatory data security assessment by the Cyberspace Administration of China, or

(b) the certification of Personal Data protection by a professional institution, or

(c) the signing of the Standard Contract.

2.2 The parties must attach the mechanism that enables the Data Importer to process the Personal Data in a foreign country to this DPA.

2.3 If any Personal Data transfer between the Data Importer and the Data Exporter requires execution of the Standard Contract, the parties will execute the Standard Contract and take all other actions required to legitimise the transfer, including filing the Standard Contract with the competent authorities, or implementing any necessary supplementary measures.

2.4 The Data Importer will not transfer any Personal Data to another country unless the transfer complies with Data Protection Laws.

2.5 The Data Exporter must obtain and maintain all applicable regulatory filings, approvals, consents, and certifications from the relevant PRC authorities for the transfers of Personal Data collected and generated by the Data Exporter located in China.

3 Brazil

3.1 Where a Restricted Transfer of Personal Data originating in Brazil is subject to the Brazilian General Data Protection Law, Law No. 13,709/2018 (LGPD), the parties shall comply with the applicable requirements of Brazil's international data transfer regime, including the International Data Transfer Regulation issued by the ANPD and, where applicable, the ANPD standard contractual clauses or another valid transfer mechanism recognized by the ANPD.

3.2 To the extent the ANPD standard contractual clauses apply, the parties shall incorporate them without modification except as permitted by Brazilian law.

4 India

4.1 Where Personal Data originating in India is processed under or in connection with the Solutions, the parties shall comply with the Digital Personal Data Protection Act, 2023 and the rules, notifications and directions issued thereunder, including any restrictions on transfers to countries or territories outside India to the extent applicable to the Solutions.

5 Turkey

5.1 Where Personal Data originating in Turkey is transferred abroad under Turkish Data Protection Law No. 6698, the parties shall comply with the applicable requirements for transfers abroad, including, where applicable, the standard contract or another valid transfer mechanism recognized by the competent Turkish data protection authority or otherwise permitted under Turkish law. To the extent a standard contract applies, the parties shall execute it in the form required by Turkish law and complete any required notification or filing formalities.

6 Switzerland

6.1 Where a Restricted Transfer of Personal Data from a Data Exporter to a Data Importer is subject to the GDPR and the FADP, the following additional provisions to the EU SCCs will apply for the EU SCCs to be suitable for ensuring an adequate level of protection for such transfer in accordance with Article 6 paragraph 2 letter (a) of FADP:

(a) '**FDPIC**' means the Swiss Federal Data Protection and Information Commissioner.

(b) '**Revised FADP**' means the revised version of the FADP of 25 September 2020, which came into force on 1 September 2023.

(c) The term '**EU Member State**' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for pursuing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).

(d) The EU SCCs also protect the data of legal entities until the entry into force of the Revised FADP.

(e) The FDPIC will act as the 'competent supervisory authority' insofar as the relevant Restricted Transfer is governed by the FADP.

6.2 The parties will also comply with the additional safeguards to the EU SCCs as set out in section 6 of **Attachment D**.

7 UK

7.1 Where a Restricted Transfer of Personal Data from a Data Exporter to a Data Importer is subject to UK Data Protection Laws, this section 4 of Attachment E will apply. The parties also agree to comply with the additional safeguards to the EU SCCs as set out in section 6 of **Attachment D**.

PART 1 – TABLES

Table 1: Parties and signatures

Start date	DPA effective date	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	NTT DATA or Supplier, as applicable. See **Attachment B**.	NTT DATA or Supplier, as applicable. See **Attachment B**.
Key Contact	Please see **Attachment A**.	
Signatures (if required for the purposes of Section 2)	N/A	N/A

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed in Attachment E, including the Appendix Information.

Table 3: Appendix Information

'**Appendix Information**' means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the parties), and which for this DPA is set out in:

Annex 1A: List of Parties: The contents of Annex I.A of **Attachment D**
Annex 1B: Description of Transfer: See **Attachment B**
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See **Attachment C**
Annex III: List of Sub processors (Modules 2 and 3 only): See **Attachment B**

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party

PART 2 – MANDATORY CLAUSES

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Attachment F California Consumer Privacy Act Terms

These CCPA terms only apply where Supplier processes personal data of California residents.

1 Definitions

1.1 The following definitions apply:

(a) '**CCPA**' means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199), and any related regulations or guidance provided by the California Attorney General.

(b) '**Contracted Business Purposes**' mean the purposes for processing personal information as set out in **Attachment B**.

(c) '**Personal Information**' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

1.2 The following lower case terms used but not defined in this **0**, such as 'aggregate consumer information', 'business purposes', 'commercial purposes', 'consumer', 'de-identify', 'processing', 'pseudonymize', 'sale', and 'verifiable consumer request' will have the same meaning as set forth in §§ 1798.14 of the CCPA.

2 Supplier's CCPA Obligations

2.1 Supplier will only process Personal Information for the Contracted Business Purposes for which NTT DATA provides or permits Personal Information access, including under any 'sale' exemption.

2.2 Supplier will not process, sell, or otherwise make Personal Information available for Supplier's own commercial purposes or in a way that does not comply with the CCPA. If a law requires Supplier to disclose Personal Information for a purpose unrelated to the Contracted Business Purposes, Supplier must first inform NTT DATA of the legal requirement and give NTT DATA an opportunity to object or challenge the requirement, unless the law prohibits such notice.

2.3 Supplier will limit Personal Information processing to activities reasonably necessary and proportionate to achieve the Contracted Business Purposes or another compatible business purpose.

2.4 Supplier must promptly comply with any NTT DATA request or instruction from Authorized Persons requiring Supplier to provide, amend, transfer, or delete the Personal Information, or to stop, mitigate, or remedy any unauthorized processing.

2.5 If the Contracted Business Purposes require the collection of Personal Information from consumers on NTT DATA's behalf, NTT DATA must provide Supplier with a CCPA-compliant notice addressing use and collection methods that NTT DATA specifically pre-approves in writing. Supplier will not modify or alter the notice in any way without NTT DATA's prior written consent.

2.6 If the CCPA permits, Supplier may aggregate, de-identify, or anonymize Personal Information so it no longer meets the Personal Information definition, and may use such aggregated, deidentified, or anonymized data for its own research and development purposes.

3 Assistance with NTT DATA's CCPA Obligations

3.1 Supplier will reasonably cooperate and assist NTT DATA with meeting NTT DATA's CCPA compliance obligations and responding to CCPA-related inquiries, including responding to verifiable consumer requests, taking into account the nature of Supplier's processing and the information available to Supplier.

3.2 Supplier must notify NTT DATA immediately if it receives any complaint, notice, or communication that directly or indirectly relates to either party's compliance with the CCPA. Specifically, Supplier must notify NTT DATA within 5 working days if it receives a verifiable consumer request under the CCPA.

4 Subcontracting

4.1 Supplier may use subcontractors to provide the Contracted Business Purposes. Any subcontractor used must qualify as a service provider under the CCPA and Supplier cannot make any disclosures to the subcontractor that the CCPA would treat as a sale.

4.2 For each subcontractor used, Supplier will give NTT DATA an up-to-date list disclosing:

(a) The subcontractor's name, address, and contact information.

(b) The type of services provided by the subcontractor.

(c) The Personal Information categories disclosed to the subcontractor in the preceding 12 months.

4.3 Supplier remains fully liable to NTT DATA for the subcontractor's performance of its agreement obligations. Supplier will audit a subcontractor's compliance with its Personal Information obligations in accordance with our policies on a periodic basis and provide NTT DATA with the audit results on request.

5 CCPA Warranties

5.1 Both parties will comply with all applicable requirements of the CCPA when processing Personal Information.

Supplier warrants that it has no reason to believe any CCPA requirements or restrictions prevent it from providing any of the Contracted Business Purposes or otherwise performing under this DPA. Supplier will promptly notify NTT DATA of any changes to the CCPA's requirements that may adversely affect its performance under the DPA.