# Data Processing Agreement

## Contents

## 1 Introduction

1.1 This Data Processing Agreement ('**DPA**') forms part of the agreement between NTT DATA and Client ('**Client Agreement**') under which NTT DATA provides certain products and/or services ('**Services**') to Client.

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

## 2 Defined terms

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

2.2 '**Affiliate**' means a legal entity that controls, is controlled by, or that is under common control with either Client or NTT DATA. For purposes of this definition, 'control' means ownership of more than 50% interest of voting securities in an entity or the power to direct the management and policies of an entity.

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 '**Client**' means the entity to whom NTT DATA provides Services, as identified in the Client Agreement.

2.7 '**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 applicable Data Protection Laws.

2.8 '**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 applicable Data Protection Laws.

2.9 '**Data Protection Laws**' means any mandatory laws applicable to a party in connection with the processing of personal data under the Client 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 ('**FADP**'), (e) China Data Protection Laws and (f) any applicable laws worldwide relevant to NTT DATA or Clients (where applicable and as recipients of services provided by NTT DATA) relating to data protection.

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

2.11 '**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.

2.12 '**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.

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

2.14 '**NTT DATA**' means the member of the NTT Ltd Group who provides Services to Client as identified in the Client Agreement.

2.15 '**NTT Ltd Group**' means NTT Ltd and its Affiliates from time to time.

2.16 '**Personal Data**' means all personal data provided to NTT DATA by, or on behalf of, Client through Client's use of the Services.

2.17 '**Privacy Statement**' means the then-current privacy statement describing NTT DATA's treatment of Personal Data in its general business administration, management, and operations, which is made available at services.global.ntt (or successor site) and as may be updated by NTT DATA from time-to-time (effective upon publication).

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

2.19 '**Standard Contractual Clauses**' or '**SCCs**' means any pre-approved standard contractual clauses for the international transfer of personal data under applicable Data Protection Laws, including the EU SCCs, the Swiss Addendum and UK Addendum, 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).

2.20 '**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. An English translation of the Standard Contract is available here.

2.21 '**sub-processor**'' means any processor engaged by NTT DATA or any Affiliate that processes Personal Data pursuant to the Client Agreement. Sub-processors may include third parties (external processor) or any NTT DATA Affiliate.

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

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

2.24 **'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.

2.25 '**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.

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

2.27 **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 Applicable law

3.1 NTT DATA may be required to process Personal Data on behalf of Client under any applicable Data Protection Laws.

3.2 Unless expressly stated otherwise, in the event of any conflict between the main body of this DPA and Data Protection Laws, the applicable Data Protection Laws will prevail.

3.3 To the extent NTT DATA is a processor of Personal Data subject to the EU Data Protection Laws and/or UK Data Protection Laws, the mandatory sections required by Article 28(3) of the GDPR (or UK GDPR, as applicable) for contracts between controllers and processors that govern the processing of personal data are set out in clauses 5.1,5.2, 6.1,6.3, 6.3, 7, 8.1, 8.2, 9.1, 9.2, 10 to 13 (inclusive).

3.4 If NTT DATA is processing Personal Data within the scope of the CCPA, the CCPA Terms contained in Attachment F govern the processing of Personal Data. The CCPA Terms do not limit or reduce any data protection commitments NTT DATA makes to Client in the DPA, Client Agreement or other agreement between NTT DATA and Client.

## 4 Duration and termination

4.1 This DPA will remain in force so long as the Client Agreement remains in effect or NTT DATA retains any Personal Data related to the Client Agreement in its possession or control.

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

## 5 Personal data types and processing purposes

5.1 The Client and NTT DATA acknowledge that the Client is the controller and NTT DATA is the processor or sub-processor of Personal Data.

5.2 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 Services described in the Client Agreement ('Business Purposes'), are specified in Attachment B.

5.3 The Client 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 DATA.

## 6 NTT DATA obligations

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

6.2 **Independent controller**. To the extent NTT DATA uses or otherwise processes Personal Data in connection with NTT DATA's legitimate business operations, NTT DATA will be an independent controller for such use, will process Personal Data in accordance with its Privacy Statement, and will be responsible for complying with all applicable laws and controller obligations.

6.3 **Compliance**. NTT DATA will reasonably assist Client in complying with Client's obligations under applicable Data Protection Laws. In doing so it will take into account the nature of NTT DATA's processing and the information made available to NTT DATA, including in relation to data subject rights, data protection impact assessments, transfer impact assessments and reporting to and consulting with data protection authorities under applicable Data Protection Laws. NTT DATA will immediately notify Client if, in its opinion, any instruction infringes applicable Data Protection Laws. This notification will neither constitute a general obligation on the part of NTT DATA to monitor or interpret the laws applicable to Client, nor constitute legal advice to Client.

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

## 7 Contracting with sub-processors

7.1 **Use of sub-processors**. NTT DATA uses sub-processors which may be located outside the country where Personal Data is collected, and which will process personal data as sub-processors. Some sub-processors might make further onward transfers of Personal Data.

7.2 **List of sub-processors**. A list of NTT DATA's sub-processors that NTT DATA directly engages for the specific Services as a processor is available on request to the NTT DATA contact mentioned in **Attachment A** or as otherwise made available on an NTT DATA website.

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

7.4 **Changes.** NTT DATA will notify the Client in writing of any intended changes to the agreed list of sub-processors at least 30 days in advance, thereby allowing the Client to object to such changes. Such objection must be made in writing to the NTT DATA contact mentioned in **Attachment A** within 14 days of notification. Client's failure to submit a written objection to the agreed list of sub-processors within 14 days of notification, will be deemed acceptance of the changes to the agreed list of sub-processors.

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

## 8 Client obligations

8.1 **Data subject requests**. If NTT DATA 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 DATA is a processor or sub-processor, NTT DATA will redirect the data subject to make its request directly to Client. Client will be responsible for responding to any such request. NTT DATA 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 DATA incurs in providing this assistance.

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

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

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

## 9 Security

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

9.2 **Access to Personal Data.** NTT DATA 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 Client Agreement. NTT DATA will ensure that persons authorized to process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

9.3 **Cost negotiations**. The parties will negotiate in good faith the cost, if any, to implement material changes other than 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 NTT DATA will bear the responsibility for such cost).

## 10 Audits

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

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

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

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

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

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

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

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

Affiliates of NTT DATA are intended third-party beneficiaries of this section.

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

## 11 Incident management

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

(a) notify Client of the Security Incident;

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

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

11.2 **Security incident notification**. Notification(s) of Security Incidents will take place in accordance with clause 11.4. Where the Security Incident involves Personal Data of the Client, NTT DATA will make reasonable efforts to enable Client to perform a thorough investigation into the Security Incident, formulate a correct response, and take suitable further steps in respect of the Security Incident. NTT DATA will make reasonable efforts to assist Client in fulfilling Client's obligation under applicable Data Protection Laws to notify the relevant data protection authority and data subjects about such Security Incident. NTT DATA's notification of or response

to a Security Incident under this clause is not an acknowledgement by NTT DATA of any fault or liability for the Security Incident.

11.3 **Other incidents**. NTT DATA will notify Client promptly if NTT DATA 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 NTT DATA processes on behalf of Client and its data subjects; or

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

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

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

## 12 Cross border transfers of Personal Data

12.1 **General**. Except as described elsewhere in the DPA, Personal Data that NTT DATA processes on Client's behalf may be transferred to and stored and processed in any country in which NTT DATA or its sub-processors may operate.

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 in accordance with 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 NTT DATA and the Client requires the execution of SCCs to comply with the applicable Data Protection Law, the parties' signature to this DPA, the Client Agreement, or to any other binding document which otherwise incorporates the DPA will be considered as signature to the SCCs.

12.4 **Change of statutory transfer mechanism**. To the extent that NTT DATA is relying on the EU SCCs, UK Addendum 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, Client and NTT DATA 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 **Client deletion**. For certain Services, Client is responsible for installing, hosting, processing and using Personal Data. Here only Client can access, extract and delete Personal Data stored in that Service. Where the particular Service does not support access, retention or extraction of software provided by Client, NTT DATA has no liability for the deletion of Personal Data as described in this clause 13.1.

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

(a) related to the processing;

(b) when this DPA terminates;

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

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

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

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

## 14 Liability and warranty

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

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

16.2 **Governing law**. This DPA is governed by the laws of the country specified in the relevant provisions of the Client 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 Client 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 Client at least 14 days in advance, allowing the Client 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. Client'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/compliance officer of Client:**

Contact information: Where applicable, as set forth in the Client Agreement or information about the Client'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 Client's website or to be provided by the Client in writing.

**Contact information of the data protection officer of NTT DATA:**

Contact information: Where applicable, as set forth in the Client Agreement.

Contact Information of NTT DATA's Global Data Protection Officer: Ashleigh Meiring, Vice President, Data Privacy & Protection; privacyoffice@global.ntt

## Attachment B Particulars of Processing

**Categories of data subjects whose personal data is transferred**

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

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

**Categories of personal data transferred**

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

- Basic personal data (for example first name, last name, email address and work address);
- 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);
- Unique identification numbers and signatures (for example IP addresses);
- Location data (for example, geo-location network data);
- Device identification (for example IMEI-number and MAC address).

**Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures**

- Biometric Information (where applicable) (for example fingerprints at NTT DATA data centers)

NTT DATA will notify Client in writing to the extent NTT DATA needs to collect additional sensitive data beyond those listed above in order to provide the Services. 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).**

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

**Nature of the processing**

The Personal Data transferred may 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 NTT DATA to provide the Services under the existing Client Agreement. This may include:

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

**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.

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

See clause 7 of the DPA. A list of NTT DATA's sub-processors that NTT DATA directly engages for the specific Services as a processor is available on request to the NTT DATA contact mentioned in **Attachment A** or as otherwise made available on a NTT DATA website. Any such sub-processors will be permitted to obtain personal data only to provide some or all of the Services NTT DATA has engaged them to provide, and they are prohibited from using personal data for any other purpose.

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

As advised by Client in writing from time to time.

## Attachment C Technical and Organizational Measures

### Introduction

At NTT DATA it is our vision, through technology and innovation, to enable a secure and connected future. We have established our NTT DATA Technical and Organizational Measures ('**TOMs**') that describe how we ensure the protection of personal data in a transparent, fair, ethical and lawful way.

Our TOMs are based on industry best practices and applicable legal requirements in jurisdictions in which we operate taking into account the nature of the data we process and the cost of implementation.

If you have any questions about our TOMs or how they relate to our products, services and solutions, please contact us at privacyoffice@global.ntt

### (A) Data Privacy and Protection Measures

#### 1 Governance and Operating Model

1.1 NTT DATA is committed to demonstrating accountability when NTT DATA processes personal data and has implemented an organizational structure, roles and responsibilities for managing and providing oversight for 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 management within NTT DATA. Ultimate accountability for data privacy and protection in our business is held by the NTT Ltd. Board and is supported by designated roles throughout the business, including Data Protection Officers or equivalent roles.

1.3 NTT DATA reports on the design and operating effectiveness of its data privacy and protection activities to the NTT Ltd. Audit and Risk Committee periodically.

#### 2 Policies, Processes, and Guidelines

2.1 NTT DATA has implemented and communicated its policies, processes, standards and guidelines that detail how NTT DATA employees are expected to process personal data. This includes the following policies:

(a) Data Privacy and Protection Policy

(b) Data Subject Rights Policy

(c) Personal Data Breach Notification Policy

2.2 NTT DATA has defined and communicated privacy notices that provide information to employees, clients and other stakeholders about how personal data is processed.

2.3 NTT DATA has a Data Protection Impact Assessment ('**DPIA**') Process and performs DPIAs when required, and following applicable data protection laws.

#### 3 Data Protection By Design

3.1 NTT DATA is committed to implementing reasonable measures to support its clients' ability to comply with data protection laws. As far as possible, the principles of data protection by design and by default are applied during the development of NTT DATA products, services, and solutions.

#### 4 Data Landscape

4.1 NTT DATA has implemented processes to identify, record, assess and maintain an understanding of the personal data that it processes.

4.2 NTT DATA maintains a record of the personal data processed in accordance with applicable data protection laws.

#### 5 Information Lifecycle Management

5.1 NTT DATA 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 NTT DATA maintains a data retention policy and schedule, which is aligned with applicable laws. NTT DATA only retains personal data where there is a legitimate business purpose and in accordance with its obligations under the law. NTT DATA 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.

5.3 NTT DATA keeps the personal data processed on behalf of its clients in accordance with client requirements and will destroy, delete, de-identify or return personal data when requested and where there are no further obligations to retain the personal data under applicable law.

5.4 NTT DATA has implemented all reasonable efforts to ensure that personal data is accurate, complete and up-to-date.

## 6 Data Subject Rights

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

6.2 NTT DATA has implemented a Data Subject Rights Policy and Data Subject Requests Process to uphold the data subject rights in accordance with applicable data protection laws.

6.3 NTT DATA 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 NTT DATA maintains a record of all data subject requests received and the actions taken to respond to these requests.

6.5 NTT DATA will provide all reasonable support to clients in responding to data subject requests, where requested, and in accordance with our agreements with them.

6.6 NTT DATA is committed to ensuring that we respond to all requests from public authorities to access personal data in accordance with applicable laws, and where permitted uphold and enforce the rights and freedoms of individuals. Where requests are made of NTT DATA to disclose personal data, NTT DATA does so in accordance with its Public Authority Data Request Policy and maintains a record of these requests and publishes these in an annual transparency report.

## 7 Cross-border Transfers

7.1 NTT DATA relies on Standard Contractual Clauses to support the lawful transfer of personal data from the European Union or from the United Kingdom to third countries and has appropriate agreements in place with NTT DATA subsidiaries, affiliates, processors, sub-processors, and clients to support cross-border transfers. Where required, NTT DATA may also request consent from data subjects for the cross-border transfer of their personal data.

7.2 Where personal data is transferred across borders, NTT DATA 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, NTT DATA 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 NTT DATA is committed to keeping abreast of changes to data protection laws in the countries in which NTT DATA operates and has implemented processes to support compliance.

## 9 Training and Awareness

9.1 NTT DATA requires all NTT DATA 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. Where required, local, regional or functional training to support NTT DATA employees to act in line with the requirements in specific countries, regions or business functions.

## 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; NTT DATA has implemented appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of personal data.

10.2 NTT DATA's security methodologies are aligned to ISO 27001 and the NIST Cyber Security Framework ('**CSF**').

## 11 Breach Response and Notification

11.1 NTT DATA 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 NTT DATA is committed to ensuring that applicable data protection authorities, affected clients and affected data subjects are notified in the event of a personal data breach in compliance with applicable data protection laws and any contractual commitments.

11.3 NTT DATA maintains a record of all personal data breaches and the actions taken to respond to these events.

11.4 NTT DATA incident management measures to identify, detect, respond and recover from information security incidents are outlined in Section B below of these TOMs.

## 12 Third Party Management

12.1 NTT DATA is accountable for the actions of its processors and sub-processors who process personal data on NTT DATA's behalf. NTT DATA assesses the ability of its processors and sub-processors to protect personal data in accordance with NTT DATA standards at the time of selection and periodically thereafter.

12.2 NTT DATA processors and sub-processors are required to sign appropriate agreements that govern the processing and protection of personal data. These agreements include requirements to ensure that the same obligations are passed to any further processors who may process personal data.

## (B) Information Security Measures

NTT DATA is committed to ensuring that information security is implemented and properly managed to protect the confidentiality, integrity and availability of personal data.

NTT DATA has established a group-wide Information Security Management System ('**ISMS**') which holds an ISO 27001 certification.

## 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, including a Chief Information Security Officer and Information Security Officers throughout the business functions.

13.2 NTT DATA 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 NTT DATA has documented and published a set of information security policies that support the requirements of the ISMS. Policies and supporting documentation are reviewed periodically.

## 15 Mobile Device Management

15.1 NTT DATA has a Mobile Devices and Teleworking Policy. NTT DATA has measures in place to ensure that mobile devices (including laptops, mobile phones, tablets, devices allowing remote access and 'Bring Your Own Device' schemes) and their contents are protected. Reasonable efforts have been undertaken by NTT DATA to ensure that Mobile Device Management ('**MDM**') software is installed on all mobile devices with access to the corporate networks and client information, systems, networks and infrastructure.

## 16 Human Resources

16.1 NTT DATA has a Human Resources Policy. NTT DATA 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 client 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.

16.2 NTT DATA requires that NTT DATA employees (including contractors and temporary employees) agree to maintain the confidentiality of NTT DATA and client data (including personal data).

16.3 NTT DATA employees are required to complete information security awareness training on an annual basis. Information security policies and supporting procedures, processes and guidelines are available to employees and communicated regularly.

16.4 NTT DATA employees receive relevant information about trends, threats and best practices through NTT DATA communication platforms.

## 17 Workplace Surveillance

17.1 NTT DATA implemented a workplace Surveillance policy to implement processes and systems to protect and safeguard the Confidentiality, Integrity and Availability ('**CIA**') of all critical information (including Personal Data) and information processing assets.

17.2 The purpose of the Workplace Surveillance Policy is to inform NTT DATA Users and others when workplace surveillance may take place.

17.3 NTT DATA may conduct electronic monitoring and surveillance of Users in the place where the employee works, whether at a place of work provided by NTT DATA, at a client or at home ('**workplace**') to protect against User misconduct, manage productivity, and increase workplace safety ('**workplace surveillance**').

## 18 Acceptable Use

18.1 NTT DATA has an Acceptable Use Policy that supports the proper and effective use and protection of NTT DATA information assets, including computer and telecommunications resources, products, services, solutions and IT infrastructure.

## 19 Asset Management and Classification

19.1 NTT DATA has an Asset Management and Classification Policy that describes the appropriate controls for handling information based on its classification. Information and assets are protected in line with the classification label.

## 20 Access Controls

20.1 NTT DATA has an Access Control Policy, supporting procedures and logical and physical access measures, to ensure that only authorized persons have access to information based on the principles of least privilege.

20.2 Where reasonable, NTT DATA has applied industry-standard encryption at-rest and in-transit to ensure that personal data is protected against any unauthorized access or disclosure. Access reviews are periodically performed on IT assets, applications, systems, and databases to ensure only authorized individuals have access.

20.3 NTT DATA has undertaken reasonable efforts to strictly limit the number of privileged ('**Admin**') users on all applications, systems and databases and does not permit generic accounts or the sharing of credentials unless expressly authorized by management or NTT DATA clients.

## 21 Encryption and Key Management Policy

21.1 NTT DATA has an Encryption and Key Management Policy that supports the efficient use of encryption and encryption key management within NTT DATA to prevent unauthorized or malicious third parties from recovering the original information whether in transit or at rest. Associated standards provide guidance in the use of cryptographic controls for the protection of information.

## 22 Network Security

22.1 NTT DATA has a Network Security Policy containing measures that apply to NTT DATA networks to manage, control and protect NTT DATA information.

## 23 Application Security

23.1 NTT DATA has an Application Security Policy requiring that all NTT DATA software applications developed in-house or purchased are managed, and access to these is controlled to protect NTT DATA information as well as to ensure the in-house application development incorporates security best practices from the initial design stage of application development.

## 24 Back ups

24.1 NTT DATA has a Backup Policy that defines the requirements for maintaining and recovering backup copies of sensitive NTT DATA information created, processed, or stored on NTT DATA computers and communications systems.

## 25 System Security Policy

25.1 NTT DATA has a System Security Policy requiring that NTT DATA systems are managed and controlled to protect NTT DATA information. NTT DATA systems consist of all physical virtual systems, including servers, workstations and devices within the NTT DATA corporate offices and the NTT DATA Cloud.

## 26 Physical and Environmental Security

26.1 NTT DATA has a Physical Security Policy. NTT DATA has implemented reasonable and appropriate measures in line with the Physical Security Policy to prevent unauthorized physical access, damage or interference with our information, applications, systems, databases and infrastructure across the following domains:

(a) Physical access controls;

(b) Monitoring and auditing of physical access;

(c) Protection from environmental hazards;

(d) Securing physical assets;

(e) Cabling security;

(f) Handling of physical assets;

(g) Maintenance and disposal of physical assets;

(h) Clear desk and screen practices;

(i) Visitors access and supervision; and

(j) Health and safety procedures.

## 27 Operational Security

27.1 The NTT DATA Digital & Global Business Services ('**DGBS'**) Division is responsible for managing NTT DATA applications, systems, databases and infrastructure in line with NTT DATA Information Security Policies, Standards and Guidelines. DGBS documents, maintains and implements all IT operational policies, processes and procedures aligned to COBIT and ITIL standards.

27.2 NTT DATA has a policy and supporting procedures for secure architecture, design, operation, and maintenance to govern changes to our business processes, applications, systems, databases and infrastructure. NTT DATA operates several governance structures to review and approve changes based on the size and scope of the change and strategic objectives. All requests and their outcomes are logged and documented.

27.3 NTT DATA has a Vulnerability Management Policy and has established a threat and vulnerability management programme supported by industry-standard tools for identifying, managing and mitigating risks to company information including the personal data of employees and clients. This includes next-generation Endpoint Detection and Response ('**EDR**') for Anti-Virus and Anti-Malware tools, regular scanning of environments, patching protocols and management of remediation and improvement activities.

27.4 Capacity requirements are continuously monitored and regularly reviewed. Systems and networks will be managed and scaled in line with these reviews.

27.5 System availability includes architecture, high-availability design, and/or backups based on the risk and availability requirements for each system. The method for maintaining system availability or recovery, including the scope and frequency of back-ups is determined based on NTT DATA business requirements, including client requirements, and the criticality of the information. Monitoring of backups is performed to ensure the successful completion of back-ups, as well as manage any backup issues, exceptions or failures.

27.6 NTT DATA has an Information Security Monitoring Policy and apply reasonable efforts to maintain audit logging on applications and systems. Logs are periodically reviewed and are available for investigation purposes. Access to logs is strictly limited to authorized personnel only.

## 28 System Acquisition, Development and Maintenance

28.1 A Security Architecture and Design Policy and supporting standards and procedures to ensure that security by design principles are applied within the software development life-cycle.

28.2 NTT DATA has undertaken reasonable measures to prevent the creation or maintenance of backdoors or similar programming that facilitate unauthorized access to or authorities to access personal data or NTT DATA systems.

## 29 Third Party Management

29.1 NTT DATA has a Third-Party Information Security Policy and supporting procedures to ensure that information assets are protected when NTT DATA engages third-party service providers and/or processors. This includes requirements for data privacy, information security due diligence and information security risk assessments to be performed, to ensure:

(a) Information security requirements are clearly articulated and documented in agreements in accordance with NTT DATA's information security standards.

(b) NTT DATA service providers and processors implement the same level of protection and control as NTT DATA;

(c) Service providers and processors are required to report any suspected or actual information security incidents to NTT DATA promptly.

## 30 Information Security Incident Management

30.1 NTT DATA 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.

30.2 NTT DATA has established group-wide security operations to proactively monitor and manage all network and computing assets. This is supported by technical tools for information security incident response and recovery.

## 31 Business Continuity

31.1 NTT DATA has established business continuity and disaster recovery plans. NTT DATA has adopted a layered approach to ensure the availability of our systems and data.

## 32 Compliance

32.1 NTT DATA has established roles and responsibilities for identifying laws and regulations that affect NTT DATA business operations. Responsibility for compliance with laws and regulations are established at a group and regional level to ensure NTT DATA meets global and local requirements.

## 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 Services, 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 an EU Member State, as specified in the Client Agreement. Where no EU Member State is specified, disputes will be resolved by the courts of 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 Services provided by NTT DATA to Client (see details on front page) under the Client Agreement. **Attachment A** includes the contact person's name, position and contact details. The parties agree that their signature to the Client 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 supervisory authority of the country where the Client's registered office is located will act as the competent supervisory Authority for the purposes of Annex I.C of the EU SCCs (Competent Supervisory Authority).and will be determined by reference to the list of supervisory authorities of the EFTA EEA States found here: https://edpb.europa.eu/about-edpb/about-edpb/members_en].

### 3 C-P Transfer Clauses

3.1 Where Client is the controller and Data Exporter of Personal Data and NTT DATA 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 2 under Clause 9(a) (general written authorisation) will apply and '[Specify time period]' will be replaced with '14 (fourteen) days';

(b) For the purposes of Clause 13(a) (supervision), the relevant option set out in Clause 13(a) will apply depending on whether the Data Exporter is (i) established in an EU Member State, (ii) is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) of the GDPR and has appointed a representative pursuant to Article 27(1) of the GDPR or (iii) is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR;

(c) Option 1 under Clause 17 (governing law) will apply and the governing law will be the EU Member State specified in the Client Agreement. Where no EU Member State is specified, 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 referred to in **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 NTT DATA is the processor and Data Exporter of the Personal Data and the sub-processer is the 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), the sub-processor must provide notification of a personal data breach concerning Personal Data processed by the sub-processor to NTT DATA and not directly to the Client. Where appropriate, NTT DATA will forward the notification to the Client;

(b) For the purposes of Clause 8.9 (documentation and compliance), all enquiries from a Client will be provided to the Client by NTT DATA;

(c) Option 2 under Clause 9 (general written authorization) will apply and '[Specify time period]' be replaced with '14 days'. The parties also agree that the controller has delegated the decision making and approval authority for sub-processing to the Client for the purposes of Clause 9 (use of sub-processors). NTT DATA has the Client's general authorization (on behalf of the controller) for the engagement of the sub-processors referred to in **Attachment B** to this DPA. NTT DATA will follow the process set out in clause 7.3 of this DPA to inform Client and not the controller of any intended changes to that list. Where appropriate, the Client will inform the controller of any changes;

(d) For the purposes of Clause 10 (data subject rights), NTT DATA will notify Client and not the controller about any request it has received directly from a data subject. Where appropriate, the Client will forward the notification to the relevant controller. The authorization to respond to the request must be provided to NTT DATA by the Client on behalf of the controller.

(e) For the purposes of Clause 13(a) (supervision), the relevant option set out in Clause 13(a) will apply depending on whether Data Exporter is (i) established in an EU Member State, (ii) is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) of the GDPR and has appointed a representative pursuant to Article 27(1) of the GDPR or (iii) is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR;

(f) For the purposes of Clause 15 (obligations of the data importer in case of access by public authorities), NTT DATA will notify Client and not the data subject(s) in case of access by public authorities. NTT DATA agrees to provide information on request for access by public authorities to the Client in accordance with section 6 of this **Attachment D**. In the event that NTT DATA 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 will inform the Client and involve the Client in responding to the competent data protection authority;

(g) Option 1 under Clause 17 (governing law) will apply and the governing law will be the EU Member State specified in the Client Agreement. Where no EU Member State is specified, the governing law will be the law of the Netherlands.

(h) 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 NTT DATA is the processor and Data Exporter of Personal Data and Client 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 of an EU Member State, as specified in the Client Agreement.

## 6 Additional Safeguards to the EU SCCs

6.1 To the extent that the EU SCCs apply, the following safeguards will apply to the EU SCCs set out in this section 6 of this **Attachment D**.

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

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

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

(b) the applicable laws to which it is/are subject, including those requiring to disclose data to public authorities or 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 Personal Data by NTT DATA and the relevant sub-processor.

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

6.5 NTT DATA agrees to promptly notify the Client if, after having agreed to this DPA and for the duration of the term of this DPA, NTT DATA has reason to believe that it 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 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 Client otherwise has reason to believe that NTT DATA can no longer fulfil its obligations under this DPA (including in relation to the relevant sub-processor), Client will promptly identify supplementary measures (such as, for instance, technical or organisational measures to ensure security and confidentiality) to be adopted by itself or NTT DATA (and/or the relevant sub-processor), at Client'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 Unless prohibited by applicable law, NTT DATA agrees to promptly notify Client if it (or the relevant sub-processor to whom a transfer is made):

(a) receives a legally binding request by a public authority under applicable laws to which it (or the relevant sub-processor) is subject for disclosure of Personal Data. NTT DATA 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 the Client 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 NTT DATA (and the relevant sub-processor).

6.7 If NTT DATA (or the relevant sub-processor to whom the transfer is made) is prohibited by applicable law from notifying the Client as set out in section 6.6, NTT DATA will use its best efforts to obtain a waiver of the prohibition, to communicate as much information as possible, as soon as possible to the Client. If NTT DATA cannot obtain a waiver of the prohibition and is under a compelling legal obligation to disclose a legally binding request from a public authority, NTT DATA will provide the minimum information permitted by applicable law when responding to a request. Unless NTT DATA is legally prohibited from doing so (for example if there is a prohibition under criminal law to preserve the confidentiality of the investigation by the public authority), NTT DATA will provide the Client with any responses provided to the public authority.

6.8 NTT DATA agrees to document its (and the relevant sub-processors) legal assessment as well as any challenge to the request for disclosure and, to the extent permissible under applicable laws to which it (or the relevant sub-processor) is subject, make it available to Client. It will also make it available to the competent data protection authority upon request.

6.9 NTT DATA 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.

6.10 To the extent permissible under the applicable laws to which NTT DATA (and the relevant sub-processor) is subject, NTT DATA agrees to publish transparency reports or summaries regarding requests from public authorities to NTT DATA for access to data and the kind of reply provided, insofar publication is allowed by applicable law.

6.11 NTT DATA agrees to preserve the information under section 6.10 for the duration of the processing and make it available to the competent data protection authority upon request.

6.12 NTT DATA will comply with its Public Authority Data Request Policy governing the disclosure of Personal Data in response to requests from public authorities.

6.13 NTT DATA will inform (and will procure that the relevant sub-processor to whom the transfer is made will inform) data subjects in a transparent and easily accessible format, on its website, of a contact point authorised to handle complaints or requests and NTT DATA 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 section 1 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.

### 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 Switzerland

3.1 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 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.

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

## 4 UK

4.1 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 Client, as applicable. See **Attachment B** | NTT DATA or Client, 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:<br>☒ Importer<br>☒ Exporter<br>☐ 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 NTT DATA 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 **Attachment F** 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 NTT DATA's CCPA Obligations

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

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

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

2.4 NTT DATA must promptly comply with any Client request or instruction from Authorized Persons requiring NTT DATA 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 the Client's behalf, Client must provide NTT DATA with a CCPA-compliant notice addressing use and collection methods that the Client specifically pre-approves in writing. NTT DATA will not modify or alter the notice in any way without the Client's prior written consent.

2.6 If the CCPA permits, NTT DATA 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 Client's CCPA Obligations

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

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

### 4 Subcontracting

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

4.2 For each subcontractor used, NTT DATA will give Client 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 NTT DATA remains fully liable to the Client for the subcontractor's performance of its agreement obligations. NTT DATA will audit a subcontractor's compliance with its Personal Information obligations in accordance with our policies on a periodic basis and provide the Client 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.