NTT DATA
Trusted Global Innovator

NTT DATA Business Solutions

Data Processing Agreement (DPA)

§ 1 Preamble and Scope of Application

This Data Processing Agreement ("DPA" or "Agreement") applies when NTT DATA Business Solutions Inc. ("Contractor") processes Personal Data in the course of its services for a company who has executed a services contract with Contractor (the "Client"). This DPA governs the processing of all Personal Data in accordance with Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council (the General Data Protection Regulation - "GDPR"), the California Consumer Privacy Act (CRPA), the California Privacy Rights Act (CPRA), and State data privacy laws as agreed to by the parties in the services contract.   The DPA may be amended from time to time to address emerging and changing privacy laws. Unless otherwise stated, the terms used in this contract are applied in accordance with their definition in the GDPR. Unless expressly provided otherwise in this contract or in the applicable statutory provisions, electronic form (e.g. e-mail) shall also suffice for the submission of a written declaration.

§ 2 Subject Matter and Duration of the Contract

(1) This Agreement shall apply to all data processing activities performed by the Contractor for the Client within the scope of the service(s).

(2) Changes to the object of processing and changes to the process shall be agreed jointly between the Client and the Contractor and shall be set out in writing or in a documented electronic format.

(3) This contract is valid for an indefinite period of time and remains in force until the last service contract has expired or the either party terminates it by providing the other with 30 days' notice in writing. This Agreement may be terminated immediately by either party if the other has materially breached the terms of the Agreement and such breach is not remedied within 15 days.

§ 3 Details of the Data Processing

(1) The nature and purpose of the processing of Personal Data carried out by the Contractor on behalf of the Client are described in the respective service contracts). The Contractor is entitled to fulfil the subject of the Service Agreement in accordance with the provisions of this Agreement to carry out all necessary processing steps.

(2) The types of data concerned and the categories of data processed are described in Appendix 1 to this DPA.

§ 4 Obligation of the Contractor

(1) The Contractor shall process Personal Data only to the extent necessary for the performance of the Service Agreement(s), in accordance with this Agreement and applicable law.

(2) The Contractor shall refrain from any use and processing for private, personal or other commercial or business purposes. The Contractor shall avoid access to the Client's data as far as possible. If data access is necessary, the client is obliged to limit it to the minimum possible for the specific fulfilment of the order.

(3) The contractor is obliged to exercise the necessary care to ensure that all persons entrusted with the data processing comply with the statutory data protection provisions, process data exclusively in accordance with the client's instructions and do not pass on the data obtained from the client to third parties or use it in any other deviating manner. The Contractor ensures that all persons entrusted with the processing have been bound to data secrecy.

(4) The Contractor shall maintain technical and organizational measures described in Contractor's Security Standards (Appendix 3)

(5) The Contractor shall inform the Client without delay if the Contractor becomes aware of any breaches of the protection of the Personal Data processed for the Client (e.g. unauthorized access). The Contractor shall support the Client in complying with the reporting obligations in accordance with applicable law.

(6) Contractor maintains a US Data Protection Manager (Compliance-solutions@bs.nttdata.com) and a global Data Protection Officer (datenschutz-solutions-de@nttdata.com).

(7) Contractor shall inform the Client without undue delay in the event of serious disruptions to the operational process which create risks for the Client's Personal Data, in the event of justified suspicion of data protection violations or in the event of other irregularities in the processing of the Client's data. The same shall apply if the Contractor is of the opinion that the security measures agreed between the parties do no longer comply with the applicable legal requirements. The Contractor is aware that the Client is obliged to comprehensively document all breaches of the protection of Personal Data and, if necessary, to report them without undue delay to the supervisory authorities and the persons affected. The Contractor shall also inform the Client of the supervisory authority's control actions and measures insofar as they relate to this contract. This shall also apply if a competent authority investigates the data processing at the Contractor as part of administrative offence or criminal proceedings.

In such a case, the parties may agree on an interruption of the processing activity. The Contractor shall inform the Client of any such interruption of the processing activity. The Contractor shall notify the Client of the subsequent outcome of any inspection by the supervisory authorities or other competent authorities with regard to this Agreement. The Contractor shall rectify the identified deficiencies and shall take appropriate measures to remedy such deficiencies.

(8) If Personal Data or Personal Data storage devices of the Client are endangered by seizure, confiscation, insolvency or composition proceedings or other events or measures by third parties, the Contractor shall immediately inform the Client of these circumstances.

(9) The Contractor shall support the Client within the scope of its possibilities in fulfilling the requests of data subjects pursuant to the applicable data privacy laws.

§ 5 Responsibilities of the Client

(1) The Client is responsible for compliance with the statutory provisions of data protection law, in particular for the lawfulness of the data transfer to the Contractor and the data processing. In addition, the Client, being the Controller of the Personal Data, is solely responsible for safeguarding the rights of the data subjects pursuant to applicable data privacy laws.

(2) The Client shall inform the Contractor immediately and in full about any errors or irregularities in the processing results or data protection provisions or, for whatever reason, if he is no longer entitled to pass on the Personal Data to the Contractor. Furthermore, this duty to inform exists if he is exposed to control actions and measures of the competent supervisory or specialist authorities in the context of an administrative offence, criminal proceedings or liability claims of a data subject or a third party, insofar as these circumstances relate to or may affect this contract.

(3) If a claim is made against the Client by a data subject with regard to one of the rights defined in by law, the Client shall be independently responsible for defending this claim. The Contractor may support the Client in this matter by means of a special Agreement.

(4) The Client shall inform the Contractor of the details of the data protection officer(s) or contact person(s) for data protection and for all data protection issues arising from this Agreement as well as the respective persons authorized to issue instructions. In the event of a change or prolonged prevention of the contact person(s), details of the successors or authorized representatives shall be communicated to the contractual partner without delay.

(5) The client is obliged to treat all knowledge of the contractor's business secrets and data security measures obtained within the framework of the contractual relationship as confidential. This obligation shall remain in force even after termination of this contract.

§ 6 Instruction Rights of the Client

(1) The Contractor shall process the data made available to it in accordance with the provisions in § 4 of this DPA only in accordance with documented instructions from the Client and within the framework of Client’s services contract(s). The Client has the right and the obligation to issue instructions on the type, scope and procedure of the processing activities in relation to the service(s) provided by the Contractor.

(2) The instructions are initially determined by this DPA and the corresponding service contract(s) in § 2 . They may be subsequently amended, supplemented and / or replaced by the Client by individual instructions or in an agreed electronic format (e.g. ticket system, fax or e-mail) to the Contractor. Instructions or orders not provided for in the contract shall be treated as a request for a change in performance of the service(s), for which a corresponding change Agreement in written form is

required. Verbal instructions shall be confirmed immediately in writing or in documented electronic form; the Contractor shall be entitled to suspend the execution of an instruction until it has been confirmed.

(3) The Contractor shall inform the Client without delay if it is of the opinion that an instruction violates provisions of data protection law. The Contractor shall be entitled to suspend the execution of the relevant instruction until its legality is confirmed by the Client or it becomes a legally permissible instruction.

§ 7 Data Processing of the EU/EEA, Switzerland, and United States

Where relevant as identified in the services contract, Contractor may process personal data of Data Subjects from across the globe and data processing may be carried out by the Contractor in a third country outside the United States of America (“US”). Contractor and Client shall comply with the data protection laws of the respective countries including the following:

EU/EEA & Switzerland

If the Processing of Personal Data includes transfers from European Union (EU)/European Economic Area (EEA) or Switzerland Contractor shall comply the following requirements in accordance with article 44 et seq. GDPR:

- if the recipient, the country or territory where Personal Data are processed or accessed, ensures an adequate level of protection for the rights and freedoms of data subjects with regard to the processing of Personal Data, as determined by the European Commission; or
- if standard contractual clauses (SCCs based on Schrems II) have been agreed with the respective recipients or countries.

(4) The EU Standard Contractual Clauses (2021 version based on Schrems II decision by the European Court of Justice) will apply to Contractor’s processing of Client’s EU/EEA or Switzerland Personal Data where an international transfer takes place to a country which does not ensure an adequate level of protection for the rights and freedoms of data subjects with regard to the processing of Personal Data, as determined by the European Commission.

(5) In case of sub-processors, the Contractor must ensure that they provide an adequate level of protection for the transferred Personal Data. The Contractor must require its sub-processors to conclude data processing contracts and/or standard contractual clauses prior to the processing of Personal Data by the sub-processor, as soon as this is necessary. These contracts must resemble the data processing Agreement(s) between the Contractor and Client and ensure a similar level of data protection. For processing of EU/EEA and Switzerland Personal Data, the Contractor enforces the standard contractual clauses (2021 version based on Schrems II decision by the European Court

of Justice) against the sub-processor on behalf of the Data Controller where a direct enforcement right under data protection law is not available, which the Contractor is hereby expressly authorized to do by the Client.

United States

If the Processing of Personal Data includes the transfer from states that have comprehensive data privacy laws (currently California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee and Montana) the following shall apply:

State Privacy Laws:

The requirements of the California Privacy Rights Act (CPRA) are the baseline for compliance with State privacy law and the following applies:

(1) Contractor will not sell or share any Client data and will not retain, use, or otherwise disclose Company data for any purpose (including for any commercial purpose or other purpose outside of the direct business relationship between the Parties) other than as permitted by an agreement between the Parties or by the relevant State privacy laws. For the purposes of this section, “sell” and “share” shall have the meaning given to them in the CPRA.

(2) Client’s data is subject to Contractor’s confidentiality obligations and it will deleted or returned to Client at the end of the services unless retention is required by law or permitted by State data privacy regulation.

(3) Contractor will promptly notify Client, if Contractor determines that it can no longer meet its obligations under this DPA or an applicable State data privacy regulation.

(4) Contractor grants Client, upon written notice, an opportunity to take reasonable and appropriate steps to stop and remediate unauthorized use of Client data and agrees that Client may take reasonable and appropriate steps to help ensure that Contractor processes Company data in a manner consistent with the applicable Sate data privacy regulations.

§ 8 Technical and organizational Measures

(1) The Contractor’s internal organization satisfies the specific requirements of the relevant data protection provisions with and appropriate technical and organizational measures for a level of protection appropriate to the risk to the rights and freedoms of the data subjects which corresponds to the current state of the art for the respective processing activities.

(2) The Client shall inspect the Contractor's documented technical and organizational measures (Appendix 3) also referred to as Contractor’s Security Standards as part of a preliminary review before the data processing by the Contractor begins. If Client believes adjustments are required to these measures, taking into account the risk associated with the specific processing activity, Client shall inform the Contractor and the parties will work together in good faith to decide how to proceed. .

(3) The Client is responsible for reviewing the technical and organizational measures and confirming that they provide a level of security appropriate to the risks to the rights and freedoms of the data to be processed by the Contractor.

(4) The Contractor reserves the right to adapt the technical and organizational measures from time to time as long as the level of protection provided for the processing does not fall below the appropriate minimum level of security to comply with privacy laws. The Contractor shall inform the Client of any material changes to the Technical and Organizational Measures .

(5) The Contractor shall regularly monitor its internal processes and technical and organizational measures to ensure that the processing of the Client's Personal Data is carried out in accordance with the requirements of applicable data protection law).

§ 9 Rights of Data Subjects

(1) The rights of the data subjects arising from the collection, processing and use of their data by the contractor must always be asserted against the Client. The Client is responsible for safeguarding these rights. In particular, the Client shall be responsible for notifying the data subjects, providing information, correcting, deleting and blocking Personal Data. The Client shall inform the Contractor without delay of the necessary activities to realize such rights of data subjects.

(2) If a data subject contacts the Contractor directly, the Contractor shall immediately forward this request to the Client and refer the data subject to the Client, provided that it is possible to connect the request to the Client on the basis of the information provided by the data subject.

(3) The Contractor shall support the Client in responding to and fulfilling requests by data subjects. For example, if the Client is obliged under applicable data protection law to provide a data subject with information about the collection, processing or use of his Personal Data, the Contractor shall, upon request, provide the Client with the information required for this to the extent possible.

(4) The Contractor shall not correct, delete or restrict the Personal Data processed on behalf of the Client; such action by the Contractor is only permissible following documented instructions from the Client.

§ 10 Audit Rights of the Client

(1) The Client may obtain information provided about Contractor's processing of Client's Personal Data and Contractor's technical and organizational measures by requesting specific reasonable evidence from the Contractor or by means of self-assessments by the Contractor. For example, the evidence can be provided by the following types of information:

- System of Organizational Controls (SOC 1) or ISAE 3402 report.

- Conduct of a self-audit (current attestations, reports or report extracts from independent bodies (e.g. auditors, data protection officers, auditors, IT security department, data protection auditors, quality auditors).
- Internal company rules of conduct / processes, including evidence of compliance with the such.

(2) The Client and the Contractor can agree that evidence can also be provided by other documents / certificates.

(3) If Contractor’s control measures do not result in clarity for the Client, an audit by the Client or an auditor commissioned by the Client will be agreed upon in writing by the parties.

(4) If, in individual cases, controls by the Client or an external auditor acting on behalf of the Client are required, these may be carried out by the Client's Data Protection Officer and other parties appointed by the Client after informing the Contractor's Data Protection Officer in good time, that the measures for compliance with the technical and organizational requirements of the relevant data protection laws are suitable for processing by the Contractor. The audit takes place on the Contractor's premises during normal business hours without disrupting operations. The Contractor may make audits reports available dependent on the prior signing of a confidentiality agreement regarding the individual audit, e.g. in regards of the data of other customers and the technical and organizational measures put in place.

(5) If the Client commissions a third party to carry out the audit, the Client shall also oblige the third party in writing to maintain secrecy and confidentiality, unless the third party is subject to a professional duty of confidentiality. If the Client's auditor is in a competitive relationship with the Contractor, the Contractor has the right to request another auditor.

§ 11 Subcontractors

(1) Subcontracting mean services which are provided by a party other than NTT DATA Business Solutions Inc. (further data processors) and which relate directly to the performance of Client’s service(s) under this DPA and the Client’s service contract(s). Subcontracting business relationships do not include ancillary services used by the Contractor, e.g. in the form of telecommunications services, postal/transport services, maintenance and user services and/or the disposal of data carriers or documents as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. Contractor maintains compliant contractual regulations and control measures for the protection and security of the Client's data with outsourced ancillary services.

(2) The Contractor may engage subcontractors such as affiliated companies or external service providers (as listed in Appendix 2) to process Personal Data of the Client. If the Client has justified concerns in regards of a chosen subcontractor, Client will notify Contractor and the parties will address the concern.

(3) The Contractor will execute contracts with subcontractors involved in the data processing. These contracts shall impose confidentiality, data protection and data security obligations on the subcontractor similar to the level of data protection and security offered by this DPA. The Contractor shall on a regular basis review and verify the subcontractor's compliance with these obligations. The Client may receive from the Contractor, upon written request, an overview of the subcontractors used for the service as well as information on Contractor/subcontractor contract, the implementation of subcontractor's data protection obligations, and verification of the subcontractor controls.

(4) Any data transfer and data processing by a subcontractor of the Contractor shall not commence before the subcontractor complies with all requirements similar to this Agreement.

(5) If the subcontractor provides the agreed service for EU/EEA Personal Data, the Contractor will require the subcontract to comply with the EU's GDPR requirements including the Standard Contractual Clauses). Section 7 of this DPA shall apply accordingly.

§ 12 Deletion and Return of Personal Data

(1) After termination of the service contract or at any other time, the Contractor shall delete, destroy or return to the Client, at the Client's discretion, the Personal Data provided by the Client, the Personal Data collected, processed and/or used for the Client, the processing and usage results created by the Client as well as any copies and the documents received from the Client in connection with the contractual relationship. If the disclosure or return of the data or any copies is not possible for technical reasons (e.g. due to electronic storage on permanently installed or - insofar as permissible under data protection law - jointly used media) or if deletion/destruction is requested by the Client, the corresponding data shall be deleted by the Contractor in consultation with the Client and in compliance with data protection laws.

(2) At the request of the Client, electronically stored data shall either be provided in commercially available format on electronic data carriers or transferred online. This shall not apply to backup copies, insofar as these are required to ensure proper data processing, and to data required to fulfil statutory retention obligations. The Contractor may make these accessible to the Client at the end of the services contract.

(3) The Contractor shall confirm the deletion/destruction to the Client in writing or by e-mail.

§ 13 Final Provision

(4) Amendments or supplements to this DPA or any of its components must be made in writing. This also applies to a waiver of this formal requirement. .

(5) Notices/information, declarations of consent, declarations of approval and confirmations must be in writing and may be sent by e-mail.

(6) Should individual provisions of this DPA be invalid or unenforceable in whole or in part or become invalid or unenforceable due to a change in the legal situation t, this shall not affect the validity of the remaining provisions of the contract as a whole. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision which comes as close as possible to the purpose pursued by the invalid provision. The parties shall make a corresponding provision that meets this objective.

Appendix 1: Services

(1) Service description

Managed Service

It's an umbrella for Application Management Services (AMS), Managed Cloud Services (MCS), Maintenance and parts of our subscription business. The related services, provided to our customers, are described in detail in the global Managed Services Portfolio of NTT Data Business Solutions. NTTD Business Solutions ticket system based on SAP Solution Manager provides an up-to-date knowledge base containing entire history of customer's tickets and comprehensive information about problem and resolution contents.

Managed Cloud Services (MCS)

General term for SAP basis and infrastructure services in own Data Centers, on hyperscaler infrastructure or as remote service. It consists of full management of cloud infrastructure and technical operations of applications, which run on top of these infrastructures as well as long-term technical support and operations of applications.

The service includes in detail:

- Complete hosting of SAP application system landscapes, including development, quality assurance and production systems
- Provisioning of all application layers, i.e. database, SAP application servers and additional system components like gateway systems, Adobe Document Services and Fiori Frontend systems
- Complete technical monitoring and management of SAP Basis components
- Availability Service Level Agreement (SLA), including disaster recovery options, to meet the high expectations on application availability for company critical applications
- Close integration into customer SAP backend systems for seamless exchange of data with SAP S/4HANA, ERP, CRM and SCM

Application Management Services (AMS)

SLA based Application Support for all SAP products to resolve application faults and to assist users following ITIL best practices in terms of Incident Management, Request Fulfilment, Problem Management and Change Management (minor and emergency change requests).

The service includes in detail:

- We start with efficient, -structured organizational setup and knowledge transfer to promote quality and SLA from the very beginning through our transition service.
- Experienced SAP application consultants are involved for quality issue resolution:
  - Remedying application faults, e.g. due to incorrect master data or customizing/ configuration settings and

  - Supporting users in terms of handling and information issues
- All service processes we provide are ITIL based
- Local and global AMS service delivery is efficiently coordinated accordingly to customer support demand and individual requirements through our professional service delivery management.

SAP AMS does not have a one-size-fits-all scenario. Each company's needs are unique when it comes to SAP applications and their interplay with each other and third-party systems. However, the following end-to-end services are required as a minimum for companies and IT departments to deliver outcomes.

Application Support

- ✓ User Support
- ✓ Service Desk
- ✓ Event Management
- ✓ Service Request Fulfillment
- ✓ Incident Management
- ✓ Problem Management
- ✓ Change Request Management
- ✓ Application Stabilisation & Hypercare

Value-Add Application Management

- ✓ Functional Monitoring
- ✓ Testing
- ✓ Release Management
- ✓ Deployment Management
- ✓ Upgrades & EHP installations
- ✓ Feature Implementation

Service Management

- ✓ Proactive Coordination of all Managed Services
- ✓ Service-Level Management and Reporting
- ✓ Continuous Service Improvement
- ✓ SAP COE Consulting

Continuous Improvement & Innovation

- ✓ Idea & Innovation Management
- ✓ Business Value Creation, Innovation & Automation
- ✓ Multi-Provider Management

Advisory services. Advisory services provide guidance on strategic topics, future product roadmaps and functional / technical improvements and proactive coordination of all aspects of a project and service delivery. .

Consulting. Consulting services consist of implementation and optimization projects supporting clients with the following:

- ✓ planning, implementation and rollout of SAP technologies and individual programming.
- ✓ application consulting for both the SAP modules such as FI, CO, MM, SD and PP as well as modern cloud solutions and platforms.
- ✓ IT strategy and process consulting for the design of suitable, industry-specific solutions and the customization of process chains.
- ✓ technology consulting for the implementation of new technology topics from cloud platforms to front-end and IoT architectures**.**

(2) Data Subjects affected by the Processing

- Customers (employees of customer as well as possible end- customers affected by the use of the service by the customer)
- Suppliers
- Service providers (e.g. external consultants, external trainers, external sales agents, distributors)
- Strategic partners

(3) Data Types

The types of data processed for the performance of the service are:

- Personal master data/personal identification data (e.g. name, address, job title, company affiliation)
- Electronic identification data (e.g. IP address, electronic signature, connection/log data, cookies)
- Communication data (e.g. telephone, e-mail, PIN, password, ports, login)
- Pictures (photos, films, etc.)

(4) Frequency of the Transfer

Personal Data can be transferred during the term of the Statement of Work as required for client's service(s).

(5) Deletion Period

Personal Data can be retained for the term of the Statement of Work as directed by client .

Appendix 2: Third Party Services Providers

Third Party Service Providers

Appendix 3 - Technical and Organizational Measures for the Security of the Transferred Personal Data (Managed Services)

LINK to the new Security Standards-Technical and Organizational Measures.