Annex: Data Protection

Data Protection and Data Security Regulations (DuD-B)

1. This Annex "Data Protection and Data Security Regulations" ("DuD-B") sets out the data protection obligations of the Contract Parties arising from the (main) contract. The agreement applies to all data processing services or activities within the meaning of Art. 28 GDPR that are related to the (main) contract. The term of this agreement depends on the term of the (main) contract.
2. The DuD-B also apply to the testing or maintenance of automated processes or data processing systems (testing, maintenance and servicing of hardware or software) if the processing of the PRINCIPAL's personal data cannot be ruled out.

The DuD-B consists of:

Part 1: Annex to the processing of personal data in the order
Part 2: a) Concrete Details Relating to the Commissioned Processing and b) technical and organisational measures (TOM)

Part 1

General provisions on the processing of personal data on behalf of the controller

Section 1 – General provisions

(1) In its capacity as "Controller" within the meaning of Article 4 (7) of the General Data Protection Regulation (GDPR), the PRINCIPAL is accountable for compliance with the data protection regulations. The AGENT acts in the capacity of "Processor" within the meaning of Article 4 (8) GDPR. In addition, the AGENT undertakes to comply with all relevant data protection regulations when executing the order.
(2) If, in the framework of the order concerned, the PRINCIPAL is itself acting in the capacity of a service provider to other principals, the rights ensuing from this Annex shall in turn be enjoyed by the upstream principals.
(3) The PRINCIPAL shall implement suitable, effective and documented measures to ensure compliance with data protection regulations, in particular with regard to the detection and timely reporting of data protection violations.
(4) The AGENT shall support the PRINCIPAL in observing GDPR with respect to the protection of personal data, in particular also in the event of a potentially necessary data protection impact assessment and prior consultations.
(5) Amendments, supplements and ancillary agreements to this annex must be made in text form, unless otherwise contractually agreed.
(6) Where the AGENT culpably infringes statutory data-protection requirements in accordance with this DuD-B and/or statutory regulations, any liability restrictions possibly agreed between the contract parties shall not apply.
(7) In the event of a conflict between the provisions of this DuD-B and the underlying (main) contract, the provisions of this DuD-B shall take precedence in the absence of explicitly agreed derogations.

Section 2 – Data processing location

(1) The data will be processed principally within a Member State of the European Union or within another signatory state of the European Economic Area (EEA) Treaty. If the application of the GDPR has not been bindingly decided in one or more states of the EEA, these states of the EEA are also considered third countries in the sense of the GDPR.
(2) Data processing outside the EU/EEA countries (third countries) is generally not permitted.
(3) Each relocation to a third state requires the prior written consent of the PRINCIPAL and may also only occur if the special conditions of Article 44 et seq. GDPR are additionally satisfied.
(4) The processing and use of the PRINCIPAL's personal data shall generally take place at the AGENT's business premises. Necessary processing or use of the personal data of PRINCIPAL off the operating premises of AGENT, even if only temporarily, (e.g. via teleworking, remote access) is only permitted if company-wide or individual agreements have been concluded with the PRINCIPAL's employees.

Section 3 - Purpose limitation and right to issue instructions

(1) The AGENT processes the personal data exclusively for the provision of the contractually agreed purposes.
(2) The AGENT shall process personal data only on documented instructions from the PRINCIPAL, unless it is obliged to do so under EU law or the law of a Member State to which it is subject. In such a case, the AGENT shall inform the PRINCIPAL of these legal requirements prior to processing, unless the law in question prohibits this due to an important public interest. The PRINCIPAL may issue further instructions for the entire duration of the processing of personal data. These instructions must always be documented.
(3) The AGENT shall inform the PRINCIPAL immediately if it is of the opinion that instructions issued by the controller violate data protection regulations.

Section 4 – Immediate notifications and duty to inform following a data protection incident

(1) The AGENT shall notify the PRINCIPAL immediately of any irregularities, disruptions and violations of data protection regulations by the AGENT and/or the persons employed by the AGENT, as well as any suspicion of data protection violations in connection with the data processed by the PRINCIPAL. The AGENT warrants to support the PRINCIPAL in the course of fulfilling potential information duties under Articles 33 – 34 GDPR.
(2) The PRINCIPAL must be notified of the Data Protection Incident forthwith upon the AGENT becoming aware of the Data Protection Incident, the notification being made to the contact person for the (Main) Contract and to the Data Protection Officer/data protection contact of PRINCIPAL.
(3) The AGENT shall document every Data Protection Incident. The notification of a Data Protection Incident to PRINCPAL shall contain at least the following information:

1. a description of the nature of the Data Protection Incident and, where possible, details of the categories and approximate number of data subjects and approximate number of affected personal data records;
2. the name and contact details of the Data Protection Officer or another point of contact capable of providing further information;
3. a description of the probable consequences of the Data Protection Incident; and
4. a description of the measures which AGENT has taken, or proposes be taken, to rectify the Data Protection Incident and, where relevant, measures for mitigating the potentially detrimental impact thereof.

Section 5 – Sub-processors

(1) The AGENT shall not subcontract any of its processing operations that it carries out on behalf of the PRINCIPAL pursuant to these clauses to a sub-processor without the prior separate written consent of the PRINCIPAL. The AGENT shall submit the request for separate consent prior to engaging the relevant sub-processor together with the information required by the PRINCIPAL to decide on the consent. The list of sub-processors approved by the PRINCIPAL can be found here in Part II.

(2) If the AGENT engages a sub-processor to carry out certain processing activities (on behalf of the PRINCIPAL), this engagement must be by way of a contract that imposes the same data protection obligations on the sub-processor as those that apply to the AGENT under these clauses. The AGENT shall ensure that the sub-processor fulfills the obligations to which the AGENT is subject in accordance with these clauses and the GDPR.

Section 6 –Information, Rectification, Restriction, Erasure and Return of Data

(1) The AGENT may not autonomously, but only with appropriate, documented instructions of the PRINCIPAL, divulge, correct, erase regularly or on a particular occasion, or restrict the processing of the data which are processed by him on behalf of the PRINCIPAL.

(2) The PRINCIPAL may, subject to statutory retention periods and other opposing legal guidelines, demand the rectification, erasure, blocking (in the context of imposing a restriction on processing pursuant to Article 4 No 3 GDPR) and surrendering of personal data, also at any time during, or after expiry of, the (Main) Contractual period. The AGENT assists the PRINCIPAL in this regard and will act exclusively within the context of the issued instructions.

(3) Upon conclusion of the contractual work, the AGENT shall delete all documentation which has found its way into its possession in a data protection-compliant manner or return them to PRINCIPAL. Documents, data and copies which cannot be surrendered shall be deleted after completion of the contractually agreed performances. The deletion must be automatically confirmed in writing or in text form. Statutory retention obligations to which the AGENT is subject shall remain unaffected by this. Contract-related data which are needed for securing the evidentiary interests of AGENT may be retained in a blocked form until expiration of the limitation periods applicable for the case concerned. Until the deletion or return of the data, the AGENT shall continue to guarantee compliance with these clauses.

Section 7 - Security of processing

(1) The AGENT shall take at least the technical and organisational measures listed in Part II to ensure the security of personal data. This includes protecting data against a breach of security that results in the destruction, loss, alteration, or unauthorised disclosure of or access to the data, whether accidental or unlawful.

(2) The AGENT shall provide the PRINCIPAL with a confirmation of compliance (e.g. certificates or evidence/receipts from an audit, a data protection officer or an auditing firm regarding compliance with appropriate measures) before the start of data processing and thereafter, unless otherwise agreed in individual cases, on an annual basis without being requested to do so or shall provide this accordingly.

(3) The AGENT shall grant its personnel access to the personal data subject to processing only to the extent strictly necessary for the performance, management and monitoring of the contract. The AGENT warrants that the persons authorised to process the personal data received have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality and have been made familiar with this.

Section 8 -Documentation and compliance with the clauses

(1) The parties must be able to prove compliance with these clauses.

(2) The AGENT shall process requests from the PRINCIPAL regarding the processing of data in accordance with these clauses without undue delay and in an appropriate manner.

(3) The AGENT shall provide the PRINCIPAL with all information necessary to demonstrate compliance with the obligations set out in these clauses and arising directly from the GDPR. At the request of the PRINCIPAL, the AGENT shall also allow and contribute to an audit of the processing activities covered by these clauses at reasonable intervals or if there are indications of non-compliance. When deciding on a review or audit, the PRINCIPAL may take into account relevant certifications of the AGENT.

(4) The PRINCIPAL may carry out the inspection itself or commission an independent inspector. Audits may include inspections of the AGENT's premises or physical facilities and shall be conducted with reasonable advance notice.

Part 2

Concrete Details Relating to the Commissioned Processing and technical and organisational measures (TOM)

a) Concrete Details relating to the processing

Name of the (main) contract	
Contact details of PRINCIPAL'S data protection officer:	datenschutz@dzbank.de Tel. 069/7447 94101
Contact details of the data protection officer/contact person for data protection of the AGENT	
Specialist contact person of the PRINCIPAL	
Subject-matter of the processing	
Type of personal data	
Nature and purpose of the processing	
Categories of data subjects	

Sub-processors

Company name of the sub-processor	**Company address**	**Commissioned activity**	**Third country** (if relevant)	**Legal basis for the third country transfer** (if applicable)

b) Technical and organisational measures (TOM)

The following technical and organisational measures are bindingly agreed between the PRINCIPAL and the AGENT:

Measure	Implementation of the measure
Confidentiality (Art. 32 (1) (a and b) GDPR)	
[Admission] access control Data processing systems with which personal data are processed must not be capable of being access by unauthorised persons.	
[Machine usage] access control Measures must be taken to prevent access to data processing systems by unauthorised persons. *Not to be completed if data processing is carried out exclusively on the PRINCIPAL's systems*	
[Data] access control Measures to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorisation during and after processing: *Not to be completed if data processing is carried out exclusively on the PRINCIPAL's systems*	
Segregation control Measures to ensure that data collected for different purposes can be processed separately. *Not to be completed if data processing is carried out exclusively on the PRINCIPAL's systems*	
Pseudonymisation It must be ensured that names and other identifying features of natural persons are replaced by an identifier in order to exclude or significantly complicate the identification of the data subject.	

Integrity (Article 32 (1) (b) GDPR)	
Transmission control It must be ensured that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or during their transport or storage on data media, and that it is possible to check and establish to which bodies a transfer of personal data by means of data transmission facilities is envisaged.	
Input control It must be ensured that it is possible to subsequently check and establish whether and by whom personal data have been input into, modified in, or removed from, data processing systems. *Not to be completed if data processing is carried out exclusively on the PRINCIPAL's systems*	
Availability and resilience (Article 32 (1) (b) GDPR)	
Availability control and resilience It must be ensured that personal data are protected against destruction and loss. *Not to be completed if data processing is carried out exclusively on the PRINCIPAL's systems*	
Procedures for regular inspection, assessment and evaluation (Article 32 (1)(d) GDPR; Article 25 (1) GDPR)	
Order control It must be ensured that personal data processed on a commissioned basis are processed strictly in accordance with the instructions of the PRINCIPAL:	
Data protection management It must be ensured that the entirety of all documented and implemented regulations, processes and measures with which the data protection-compliant handling of personal data in the company is ensured are systematically controlled and monitored.	
Data protection by design and by default It must be ensured that when new data processing systems and software are introduced, the processing operations are designed at the earliest possible stage in such a way that privacy and data protection principles can be guaranteed from the outset. *Not to be completed if data processing is carried out exclusively on the PRINCIPAL's systems*	