Supplementary Terms and Conditions on Data Protection - Data Processing Agreement (ZB/D)

Appendix _____ to the contractual relationship (no. of the framework agreement, if available) _____ between _____ (Client) and _____ (supplier).

The Processing of personal data takes place within the frame of Data Processing in the sense of Artt. 4 No. 8 in conjunction with 28 EU-GDPR

1. Object and duration of the order

1.1. Object of the order

The object of the order results from _____ (*Service Agreement e.g. individual agreement, framework agreement, service agreement*) concerning the following commissioned service provision: _____ (*please insert short description of the services commissioned in the contract or the title of the service agreement*) of _____ (*date*) to which reference is made herein (hereinafter referred to as "Service Agreement").

1.2. Duration of the order

The duration of this order (term) corresponds to the term of the Service Agreement / The Order or Contract will be authorised for one time execution only / The Duration of this Contract is limited to _____.[1]

A premature termination of the term without period of notice shall be admissible in case of violation of legal or contractual data protection provisions. The same shall also apply if the Supplier does not want to or cannot execute a reasonable instruction of the Client.

2. Substantiation of the order content

2.1. Nature and purpose of the planned Processing of data

☐ The nature and purpose of the Processing of personal data by the Supplier for the Client are concretely described under _____[2] in the Service Agreement of _____ (date). The commissioned services relate to _____ (*please insert short description of content of commissioned services and of purpose for collecting, processing and using of data in one or two sentences*).

or

☐ Detailed description of the Subject Matter with regard to the Nature and Purpose of the services provided by the Supplier: _____.

Location of service provision

☐ The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled.

or

☐ [3]The adequate level of protection in _____ (e.g. country, territory or specific sectors within a country)

- ☐ is the result of Standard Data Protection Clauses (Article 46 Paragraph 2 Points c and d GDPR)[4];
- ☐ has been decided by the European Commission (Article 45 Paragraph 3 GDPR)[5];
- ☐ is the result of approved Codes of Conduct (Article 46 Paragraph 2 Point e in conjunction with Article 40 GDPR);
- ☐ is the result of an approved Certification Mechanism. (Article 46 Paragraph 2 Point f in conjunction with Article 42 GDPR).
- ☐ is established by other means: _____ (Article 46 Paragraph 2 Point a, Paragraph 3 Points a and b GDPR).

2.2. Type of data

The Subject Matter of the Processing of personal data comprises the following data types/categories (List/Description of the Data Categories):

- ☐ name, title, academic degree
- ☐ professional, industrial or business designation
- ☐ address
- ☐ date/year/day of birth[6]
- ☐ communication data (e.g. telephone, e-mail)
- ☐ telecommunications data (traffic data, location data, inventory data, single connection data),
- ☐ Telemedia data (usage data and inventory data) or electronic communication data (electronic communication content and electronic communication metadata)
- ☐ consumption data and network state from network and metering point operation
- ☐ contract reference data (contractual relation, product and/or contract interest)
- ☐ customer history

[1] Please delete as applicable.
[2] Please indicate the paragraph/point of the contract.
[3] To be completed by the contractor.
[4] So-called EU Standard contractual clauses „Controller to Processor". Agreement and signature of the EU Standard Contractual clauses is Client´s general requirement in the case of the Supplier planning to provide services from a so-called third country, i.e. a country outside the EU/EEA.
[5] This is the case for countries which the EU Commission has determined as having an adequate data protection level.
[6] Please delete where inapplicable.

- ☐ contract billing and payments data
- ☐ Special types of personal data (information on racial and ethnic origin, political opinions, religious or philosophical beliefs, membership in trade unions, health or sexual life, biometric data, genetic data, data about criminal convictions and criminal offences)
- ☐ personal data on bank and credit card accounts
- ☐ planning and control data (e.g. personnel operational planning)
- ☐ inquiry information (of third parties, e.g. credit agencies or of public registries)
- ☐ Other: .....

2.3. Categories of data subjects

The categories of data subjects comprise:

- ☐ employees
- ☐ relatives of employees
- ☐ pensioners/survivors
- ☐ applicants
- ☐ customers
- ☐ employees of external companies
- ☐ interested persons
- ☐ tenants/landlords, lessees/lessors
- ☐ suppliers
- ☐ contact persons
- ☐ Children (i.e. persons under age)
- ☐ Other: .....

3. Technical and organisational measures

Before the commencement of Processing, the Supplier shall document the execution of the necessary technical and organisational measures and, where applicable, operating security in accordance with Article 4 Directive 2002/58/EU and Directive 2009/136/EU], set out in advance of the order, specifically with regard to the detailed execution of the contract, and prior to the Processing, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the documented measures become the foundation of the order. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of Processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. [Details in Appendix 1]

The Supplier undertakes to comply with the following technical and organisational measures and, where applicable, operating security in accordance with Article 4 Directive 2002/58/EG and Directive 2009/136/EG:

☐ The supplementary terms and conditions on data protection – technical and organisational measures (ZB/MD) attached as an annexe shall be defined as binding for the Supplier.

☐ Instead of the ZB/MD, the Supplier may realise an order-related documentation of the technical and organisational measures in exceptional cases after coordination with the Client.

The technical and organisational measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be mutually agreed and documented.

4. Correction, restriction and erasure of data

With the exception of the rules under point 11 of these supplementary terms and conditions, the Supplier may not on its own authority rectify, erase or restrict the Processing of data that is being Processed on behalf of the Client, but only on documented instructions from the Client. Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of Processing, the Supplier will immediately forward the Data Subject's request to the Client.

Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

5. Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

[7] a) The Supplier shall appoint the competent data protection officer or – if no data protection officer is necessary – a contact person for data protection towards the Client.

☐ The appointed data protection officer/contact person of the Supplier is:
☐ The appointed contact person for data protection of the Supplier is:

_____
Name, first name, tel.

Any change of the data protection officer/contact person shall be immediately notified to the Client in writing.

[8] b) As the Supplier is established outside the EU & EEA it designates the following Representative within the Union pursuant to Article 27 Paragraph 1 GDPR: _____ [*enter: given name, surname, organisational unit, telephone, e-mail*].

c) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR and, if applicable, also the privacy of telecommunications[9] as well as confidentiality about electronic communication

[7] To be completed by the contractor.

[8] To be completed by the contractor.

data. The Supplier entrusts only such employees with the Data Processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not Process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law. The resulting secrecy obligation shall apply beyond the end of the contract for an undetermined period of time regardless of the provision on other secrecy obligations. The same applies to data which are subject to the privacy of telecommunications.

d) Implementation of and compliance with all Technical and Organisational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR.and, where applicable, operating security in accordance with Article 4 Directive 2002/58/EG and Directive 2009/136/EG].

e) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

f) The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the Processing of personal data in connection with the Processing of this Order or Contract.

g) Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract Data Processing by the Supplier, the Supplier shall make every effort to support the Client.

h) The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that Processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

i) Demonstrability of the technical and organisational measures taken towards the Client within the frame of his control rights according to Section 8 of this Data Processing Agreement.

j) Notification of the Client by the Supplier about the existence of rules and regulations for the Supplier´s employees and agents about “mobile working”, e.g. about being able to work outside of commercial units of the Supplier or subcontractor (according to Section 6 of this DPA).
Obtaining of the approval of the Client for the Processing of data of the Client out of commercial units of the Supplier or subcontractor.
Any Processing of data for the Client outside the commercial units of the Supplier/subcontractor shall only be admissible with the approval of the Client in individual cases.

6. Subcontractual relations

Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include the following ancillary services; namely telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of Data Processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

The Supplier may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Client.

a) ☐ The Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

[10]Company subcontractor	Address/country	Service

b) ☐ Outsourcing to subcontractors and/or
☐ Changing the existing subcontractor

are permissible when:

- The Supplier submits such an outsourcing to a subcontractor to the Client in writing or in text form with appropriate advance notice; and
- The Client has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Supplier; and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

The transfer of personal data from the Client to the subcontractor and the subcontractors commencement of the data Processing in the cases of Point a) or Point b) shall only be undertaken after compliance with all requirements has been achieved.

c) ☐ Subcontracting is not permitted.

d) Further outsourcing by the subcontractor

☐ Is not permitted;

☐ Requires the express consent of the main Client (at the minimum in text form); the granting of approval is at minimum dependent on the fact that all contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor. The Supplier has to prove this to the main Client in an adequate form.

[9] Acc. to. ePrivacy-Directive in its respective applicable in conjunction with national regulations as to the secrecy of telecommunications, e.g. Section 88 TKG (for Germany)

[10] To be completed by the contractor.

7. Persons authorized to give instructions on Client-side

The Client nominates the following person(s) as having the power to instruct the Client and act as contact persons for questions on data privacy and data protection in the context of this order or contract, and who will establish a contact link to the Data Protection Officer of the Client if required:

_____
Name, first name, tel.

Any change of this (These) persons shall be immediately notified to the Supplier in writing.

8. Supervisory powers of the Client

The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR. The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

[11]Evidence of such measures, which concern not only the specific Order or Contract, may be provided by

- ☐ Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
- ☐ Certification according to an approved certification procedure in accordance with Article 42 GDPR;
- ☐ Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor)
- ☐ A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification e.g. ISO/IEC 27001).

9. Notification in case of violations of the Supplier

The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the Processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

b) The obligation to report a personal data breach immediately to the Client regardless of who caused the data breach (including cases of loss of or unlawful transfer of or unlawfully gaining knowledge of personal data).

c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.

d) Supporting the Client with its data protection impact assessment .

e) Supporting the Client with regard to prior consultation of the supervisory authority.

10. Authority of the Client to issue instructions

The Client in principle issues instructions in writing (at the minimum in text form). In case as an instruction by the Client is issued only orally, the Supplier shall request confirmation of the instruction at the minimum in text form from the Client.

Section 5 Point c) sentence 3 of this Data Processing Agreement applies.

The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

11. Deletion of data and return of data carriers

The Supplier shall not Process the data for any other purposes and is in no way entitled to transfer the data to third parties. Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly Data Processing, as well as data required to meet regulatory requirements to retain data.

After the completion of the contractual works or earlier upon request by the Client – at the latest at the end of the Service Agreement – the Supplier shall return any documents received, prepared Processing and use results as well as data inventories related to the contractual relation to the Client or destroy them in accordance with data protection provisions with the Client's approval. The same shall apply for test and rejected materials. The deletion log shall be submitted to the Client on demand
Documentation serving for the evidence of the Data Processing in accordance with the order and proper Data Processing shall be kept by the Supplier in accordance with the respective storage periods even beyond the end of the contract. The Supplier may hand this over to the Client at the end of the order for the purpose of exoneration to relieve the Supplier of this contractual obligation.

_____ Place, date	_____ Place, date
_____ Signature and company seal Client	_____ Signature and company seal Supplier

[11] Auszufüllen durch den Auftragnehmer.