Annex: Data Protection

Data Protection and Data Security Regulations (DuD-B)

DZ BANK AG
Deutsche Zentral-Genossenschaftsbank,
Frankfurt am Main
Platz der Republik
D-60325 Frankfurt am Main

("PRINCIPAL")

and
…
…
…

("AGENT"),

agree the following Data Protection Annex:

1. This Annex "Data Protection and Data Security Regulations" ("DuD-B") concretises the data protection obligations of the Contract Parties arising from the (Main) Contract. Other legal and, in particular, supervisory obligations remain unaffected by this Annex. It is valid for all performances and activities which are connected with the (Main) Contract, and for which coworkers of AGENT or third parties charged by AGENT come into contact with personal data of PRINCIPAL. The period of validity of this Annex is orientated towards the period of validity of the (Main) Contract.

2. DuD-B applies additionally to the inspection and maintenance of automated procedures or data processing facilities (inspection, maintenance and servicing of hardware and / or software) if, in doing so, processing – notably access to personal data – cannot be ruled out.

3. If PRINCIPAL or a performance-receiving company within the PRINCIPAL's group of companies is an institution within the meaning of Section 1 (1 b) of the German Banking Act (Kreditwesengesetz, KWG), the regulations of this Annex shall apply mutatis mutandis for also all other data processed on a commissioned basis. This is necessary to attain an equivalent protection of all data, to uphold banking secrecy and, in the framework of the special organisational obligations, to ensure appropriate and effective risk management within the meaning of Section 25a KWG.

DuD-B consists of:

Part 1: Concrete Details Relating to the Commissioned Processing

Part 2: General Regulations in Connection with Commissioned Processing

Part 3: Agreement on the Definition of the Technical and Organisational Measures (TOM)

Part 1

Concrete Details Relating to the Commissioned Processing

Pursuant to Article 28 (3) of the General Data Protection Regulation (GDPR), the following concrete details must be specified for the commission, unless they have already been provided for in the (Main) Contract and / or its Annexes.

[COMPLETION TIP to be deleted:

Completion tip to be deleted: The following details must be specified individually for each DZ BANK Group company.]

1. Purpose of commission

AGENT processes personal data under commission by PRINCIPAL.

☐ The purpose of the commission is evident from the details of the (Main) Contract, to which reference is herewith made. Provided that the tasks of AGENT are referred to in the (Main) Contract, the contractual provisions concerned constitute a central element of this commission.

[Completion tip to be deleted: In the performance description, the commission for processing personal data must be described using simple linguistic means so that AGENT can understand why and for what purpose it is actually being commissioned by PRINCIPAL. The detailed description of the tasks to be fulfilled by AGENT is given in sub-section 3b.

2. Duration of assignment

☐ The period of this commission (duration) corresponds to the duration of the (Main) Contract.

or (notably, if the (Main) Contract does not provide for a specific duration)

☐ The commission is awarded for once-only execution and terminates as soon as the performance has been rendered respectively formally accepted.

or

☐ The period of this commission (duration) is limited until ***[Completion tip to be deleted: <date> to be entered by specialist division].***

or

☐ The commission is awarded for an unlimited period of time and can be terminated by either Contract Party with a notice period of ***[Completion tip to be deleted: <time period> to be entered by the specialist division]*** before

the end of ***[Completion tip to be deleted: <date> to be entered by the specialist division]***. The possibility of immediate termination remains unaffected hereby.

3. Nature and purpose of the processing of data

a) Purpose of the processing

☐ IT operating / hosting of application (data centre)	☐ Destruction of paper-based data media
☐ Printing of account statements	☐ Payroll accounting
☐ Market and opinion research	☐ Securities processing
☐ Telephone surveys	☐ Data / application migrations
☐ Data archiving	☐ Evaluations
☐ Payment-system processes	☐
☐	☐

[Completion tip to be deleted: The items in the above list only serve as examples and are thus not exhaustive. If the purpose of a commission is not stated here, the necessary details must be provided plausibly and comprehensively in the empty fields .]

A partial repetition of the information stated under № 1 might occur here, depending on the concrete project concerned. As such a redundancy is stipulated by the relevant legal texts, it must be accepted.]

b) Nature of the processing (description of the individual processing steps)

To fulfil his tasks and render his services in accordance with this commission, AGENT executes the following work steps:

[Completion tip to be deleted: A detailed description of the individual work steps in which the AGENT processes personal data. Care should be taken to avoid formulations which are insufficiently precise here. This is important to avoid the risk of e.g. the data protection supervisory authorities classifying the commission as other than "commissioned processing".

Negative example: "Assumption of HR admin duties".

Positive example: "Assumption of the following HR admin duties": (detailed descriptions of all assigned duties must be stated here, including information about the time, scope and the respective circle of persons (data subjects) affected by the work (see № 5)]

Example of a detailed description:

The AGENT will save the data provided by the PRINCIPAL (see Nº 4 below, "Nature of the data") in his systems and, based on a sample text supplied to him, prepare the letters to the employees (see Nº 5 below, "Circle of data subjects"), print them out on the company stationery entrusted to him, and add the job description concerned. Once the letters have been produced, the AGENT will hand over the letters to the PRINCIPAL. The USB stick that was entrusted to the AGENT will be returned to the PRINCIPAL at the same time as the handover of the produced letters. Moreover, at the end of the commission, the AGENT will destroy / erase in a data protection-compliant manner all the data and documentation that had been entrusted to him and confirm this to the PRINCIPAL, unbidden, in writing.

4. Nature of the data

AGENT will process the following types / categories of data in connection with rendering the aforementioned performances.

[Completion tip to be deleted: Detailed description of the types / categories of data:

Examples:
- ***First name;***
- ***Last name;***
- ***Street;***
- ***Postal code;***
- ***Town;***
- ***Salutation;***
- ***Salutation designation;***
- ***Date of birth / date of formation;***
- ***Personal ID number;***
- ***Client advisor;***
- ***Telephone, private;***
- ***Telephone, business;***
- ***Fax.***

Self-explanatory generic categories can also be formed and used (e.g. address data etc.]

5. Categories of data subjects

The categories of persons affected by the handling of their personal data in the framework of this commission encompass:

[Completion tip to be deleted: Precise description of the affected circles of persons

– Example descriptions:

- Customers;
- Prospective customers;

- Subscribers;
- Employees within the meaning of § 26 (8) BDSG (revised);
- Suppliers;
- Commercial agents;
- Contact persons.]

6. Scope of authority to issue instructions, competent contact persons of each Contract Party

AGENT may, for the duration of the commission, process the personal data exclusively for the purposes set out in № 1 and in accordance with the processing steps set out in № 3 Letter b), but only if and to the extent that he does so in compliance with the guidelines on protecting personal data. AGENT shall additionally follow all further concrete and / or general written instructions issued by PRINCIPAL in regard to the nature, scope and procedure of the data processing in accordance with this DuD-B.

The persons authorised to issue instructions on behalf of PRINCIPAL are: ***[Completion tip to be deleted: Please enter: name, organisational unit, function, telephone number].***

The persons authorised to receive instructions on behalf of AGENT are: ***[Completion tip to be deleted: AGENT please enter: name, organisational unit, function, telephone number].***

[Completion tip to be deleted:

- ***Persons authorised to issue instructions on behalf of PRINCIPAL could be: coworkers working for PRINCIPAL who – in connection with a project, or in connection with the scope of duties that has been respectively assigned to them in their business divisions – are responsible for this and are authorised to access the personal data. More than one person with the authority to issue instructions may also be nominated by PRINCIPAL at any one time.***

- ***Persons authorised to receive instructions on behalf AGENT could be: coworkers working for AGENT who – in connection with a project, or in connection with their scope of duties – are responsible for handling the commission and are authorised to access the personal data. More than once person with the authority to receive instructions may also be nominated by AGENT at any one time.]***

The Corporate Data Protection Officer of PRINCIPAL is:

datenschutz@dzbank.de, Tel. +49 (0)69/7447 94101

The Corporate Data Protection Officer of AGENT is:

[Completion tip to be deleted: Please complete the contact details].

In the event of a change, or longer-term hindrance, of a contact person and / or Data Protection Officer, the respective other Contract Party must be informed forthwith in writing of the successor or representative.

7. Consent to the commissioning of subprocessors

Are no subprocessors stated below, AGENT is prohibited from engaging one or more subprocessors.

AGENT may deploy the following subprocessor(s):

-

-

The above-named subprocessor(s) will be charged with rendering the following performances:

-

-

8. Validity of the Annex “Data Protection and Data Security Regulations” (DuD-B)

DuD-B is an integral part of the (Main) Contract between the Contact Parties.

Part 2

General Regulations in Connection with Commissioned Processing

Section 1 – General provisions

(1) In its capacity as “Controller” within the meaning of Article 4 (7) of the General Data Protection Regulation (GDPR), PRINCIPAL is accountable for compliance with the data protection regulations. AGENT acts in the capacity of “Processor” within the meaning of Article 4 No. 8 GDPR. Moreover, AGENT undertakes to comply with all pertinent statutory data protection regulations in the framework of executing the commission.

(2) If, in the framework of the commission concerned, PRINCIPAL is himself 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) AGENT confirms and assures that persons charged with executing the commission have been obligated in documented form to uphold confidentiality, and that they have been instructed in the data protection regulations of, in particular, GDPR and possibly in other pertinent national confidentiality guidelines (such as, but not limited to, Section 88 of the German Telecommunications Act (Telekommunikationsgesetz, TKG) and Sections 203 and 206 of the German Criminal Code (Strafgesetzbuch, StGB)). Upon PRINCIPAL’s request, AGENT shall evince said undertaking and instruction.

(4) AGENT shall implement suitable, effective and documented measures which ensure observance of the statutory data protection guidelines, notably with respect to the recognition and timely notification of data-protection breaches.

(5) AGENT shall inform PRINCIPAL without undue delay of the respective possibilities of contacting his Data Protection Officer, provided that one must be appointed under the pertinent regulations, or his data security contact. Following a change in office of the Data Protection Officer or data security contact, AGENT shall inform PRINCIPAL forthwith of the changed contact details.

(6) AGENT shall support 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

(7) With respect to the processed data and associated data media, AGENT may not plea a right of retention within the meaning of Section 273 of the German Civil Code (Bürgerliches Gesetzbuch, BGB) vis-à-vis PRINCIPAL.

(8) Amendments, supplements and collateral agreements instructions to this Annex must be made in writing. This applies likewise to this written form requirement. With respect to the execution of this Annex, amendments, supplements and collateral agreements, as well as the consent of PRINCIPAL concerning the charging of subprocessors, written form may also be satisfied by the use of an electronic format offered by PRINCIPAL pursuant to Article 28 (9) GDPR, such as an electronic ordering and ticket system.

(9) Where 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.

(10) 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. Where the use of GDPR has not been endorsed as binding in one or more states of the EEA, these states of the EEA shall also be deemed third states within the meaning of GDPR.

(2) Data processing outside the EU / EEA states (third states) is principally prohibited. This also applies to subprocessors, whereby it is noted that the term “processing” shall also mean the possibility of inspection, e.g. in the framework of remote maintenance accesses.

(3) Each relocation to a third state requires the prior consent of 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 personal data of PRINCIPAL shall take place principally on the operating premises of AGENT. Necessary processing or use of the personal data of PRINCIPAL off the operating premises of AGENT, even if only temporarily, (e.g. via teleworking or by means of remote access) is only permitted if company agreements or individual agreements satisfying the pertinent data-protection and data-security guidelines have been entered into with the staff of AGENT.

Section 3 – Authority to issue instructions, reservation of purpose

(1) When processing personal data, AGENT will be acting for PRINCIPAL and to this extent undertakes to process the data exclusively for rendering the contractually agreed performances and for the purposes of PRINCIPAL, and to follow the instructions of PRINCIPAL in doing so.

(2) The instructions must be documented and held in a suitable form.

(3) Where the (Main) Contract provides for a specific form of issuing instructions (e.g. ticket systems or e-mail), this form shall suffice.

(4) Copies and / or duplicates of the personal data shall not be prepared without the cognisance of PRINCIPAL. Excluded herefrom are backup copies, provided that these are needed for ensuring proper data processing, and data needed to conform with statutory retention duties.

(5) Verbally communicated instructions are only permissible where a delay could potentially compromise the security of personal data. Such verbally communicated instructions must be confirmed by AGENT forthwith and documented in accordance with Section 3 (2) of this DuD-B.

(6) AGENT shall notify PRINCIPAL forthwith if he opines that a work directive issued by PRINCIPAL is in contravention of data protection guidelines.

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

(1) AGENT shall notify PRINCIPAL of, and identify remedies for, irregularities in the data processing workflow, founded suspicions of violations of statutory data-protection guidelines and contractual agreements entered into between the Contract Parties concerning the protection of personal data, breaches of statutory data protection regulations by AGENT or by his engaged personnel, as well as objections raised by a data protection supervisory authority or in any other audit reports (“Data Protection Incident”) provided that he is not prevented from so doing by an official guideline in the framework of preliminary investigations. AGENT warrants to support PRINCIPAL in the course of fulfilling potential information duties under Articles 33 – 34 GDPR.

(2) PRINCIPAL must be notified of the Data Protection Incident forthwith upon 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 (datenschutz@dzbank.de).

(3) AGENT shall document every Data Protection Incident.

The documentation and 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.

Moreover, AGENT shall furnish PRINCIPAL with all information in his ambit which PRINCIPAL needs to fulfil his own notification duties.

(4) AGENT shall inform PRINCIPAL forthwith if there is a possibility of PRINCIPAL's ownership of the data residing on AGENT's premises being, or foreseeably being, compromised by way of third-party measures (e.g. seizure or sequestration), insolvency or settlement proceedings or other events.

Section 5 – Subprocessors

(1) The deployment of subprocessors by AGENT and / or further subprocessors (cascading commissioning) is only permitted with the prior written consent of PRINCIPAL.

(2) PRINCIPAL reserves the right to issue his consent only after AGENT has disclosed the name and address of the subprocessor. PRINCIPAL further reserves the right to issue his consent only if AGENT has demonstrated that his choice of subprocessor was made diligently after careful consideration of the suitability of the technical and organisational measures taken by the subprocessor.

(3) The contractual arrangements to be agreed between AGENT and the subprocessor in writing must be made in such a way as to be conformant with the provisions of this Annex. For this purpose, the technical and organisational measures to be agreed with the subprocessor must, notably, exhibit an equivalent level of security; the rights to issue instructions must be preserved without restriction and the data processing must, in accordance with Section 2 (1) of this Dud-B, fundamentally continue to be conducted in EU / EEA states in which the application of GDPR has been bindingly ratified. PRINCIPAL must be authorised to conduct controls on site at the subprocessor or to charge third parties with conducting such controls. AGENT must check regularly for compliance with the obligations.

(4) Upon PRINCIPAL's request, AGENT shall furnish information about the implementation of the data protection-relevant obligations, if necessary by enabling inspection of the relevant contractual documents.

(5) If AGENT avails himself of a subprocessor for rendering the performance for PRINCIPAL, AGENT shall, promptly upon request, furnish PRINCIPAL access to the documentation and results of the initial inspection and regular inspections conducted by AGENT in regard to the subprocessor, respectively the confirmations of the subprocessor's conformance.

(6) AGENT's scope of responsibility for the fulfilment of the activities he assigns to the subprocessor shall be the same as if AGENT had performed the activities himself. If the sub-

processor fails to fulfil his data protection obligations, AGENT shall be held liable vis-à-vis PRINCIPAL for fulfilment of the obligations of every other subprocessor.

Section 6 – Right to request, Rectification, restriction, erasure and return of data

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

(2) 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. AGENT will assist PRINCIPAL in this regard and act exclusively within the context of the issued instructions.

(3) Where a data subject approaches AGENT directly with respect to the rights of data subjects under GDPR, AGENT shall refer this request without undue delay to PRINCIPAL and wait for further instructions from PRINCIPAL.

(4) Upon conclusion of the contractual work, AGENT shall erase in a data protection-conformant manner, or return to PRINCIPAL, all documentation which he has acquired and are connected with the commission relationship – such as test material, discarded material, data backup copies and created processing results. Documents, data and copies which cannot be surrendered shall be erased after completion of the contractually agreed performances. The erasure shall be confirmed by suitable means upon request. Statutory retention periods which AGENT must observe, notably for compliance with the German Fiscal Code (Abgabenordnung, AO) and German Commercial Code (Handelsgesetzbuch, HGB) are not affected hereby. Contract-related data (such as, but not limited to, contacts of PRINCIPAL) 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.

Section 7 – Technical and organisational security measures pursuant to Article 32 GDPR

(1) AGENT will take technical and organisational measures to protect personal data against misuse and loss (data security) which are appropriate for the nature of the personal data or categories of data to be protected (see Part 3 of this Annex).

(2) When communicating by e-mail, the Contract Parties shall safeguard confidentiality by protecting confidential information against unauthorised access and manipulation.

(3) Before processing commences, AGENT shall document the implementation of the required technical and organisational measures which notably relate to the concrete execution of the commission and were expounded prior to the awarding of the commission, and submit this documentation to PRINCIPAL for inspection.

(4) AGENT may only grant [data] access rights to persons involved in executing the commission. Said access rights may only be granted to the extent needed for executing the tasks concerned. Upon PRINCIPAL's request, AGENT shall name the persons with [data] access rights, as well as the access rights granted to them.

(5) AGENT warrants that the processed data are kept strictly separate from other datasets.

(6) AGENT is, without PRINCIPAL's written consent, not authorised to connect hardware to, or install software on, systems belonging to PRINCIPAL.

(7) AGENT is not permitted to load personal data on to systems of third parties within the meaning of Article 4 No 10 GDPR insofar as AGENT has not issued any explicit instruction so to do. This is also applicable to testing purposes.

(8) The agreed measures will evolve to reflect technical progress and further developments, and must be maintained by AGENT such that they remain in a state-of-the-art condition.

This also applies for orders issued by the competent supervisory authorities. Intended significant modifications (such as, but not limited to, fundamental changes in encryption techniques or sign-on procedures) shall be documented and communicated to PRINCIPAL and, by mutual consent, set forth in an amended version of DuD-B, Part 3, TOMs, whereby PRINCIPAL shall not object to modifications without cause.

Section 8 – Enabling checks, provision of information

(1) AGENT agrees that PRINCIPAL may at any time, either himself or through a third party, verify compliance with the data protection guidelines and contractual agreements in the necessary scope, and do so, notably, by gathering information and inspecting the stored data and data processing programs, as well as by way of other checks, on location. AGENT warrants that he will cooperate in these inspections where necessary. Costs which arise in the course of such verifications will not be reimbursed.

(2) Independently thereof, AGENT shall grant PRINCIPAL and PRINCIPAL's authorised agents visitation, inspection, information and control rights (auditing rights) with respect to the agreed technical and organisational measures, fundamentally, however, subject to prior agreement with AGENT and during AGENT's customary business hours. AGENT undertakes to provide the necessary assistance in the event that inspections are demanded. Moreover, AGENT shall grant to any persons performing audits or other measures [admission] access to all his premises and properties for the purpose of enabling PRINCIPAL to observe his statutory auditing obligations.

(3) AGENT shall review regularly his internal processes as well as his technical and organisational measures to ensure that the processing in his sphere of responsibility complies with the requirements of prevailing data-protection law and that the protection of the rights of data subjects is guaranteed. AGENT shall evince his conformance with the technical and organisational measures by means of suitable proof such as, but not limited to, evidence from his auditing function, his company Data Protection Officer or a recognised public statutory auditor (Confirmation of Compliance).

(4) AGENT shall present and make available to PRINCIPAL the Confirmation of Compliance before the start of the data processing and, in the absence of individual, alternative arrangements, thereafter unbidden annually.

Part 3

Agreement on the Definition of the Technical and Organisational Measures (TOM)

Agreement on the Definition of the Technical and Organisational Measures

AGENT shall implement appropriate technical and organisational measures (Article 32 GDPR) to ensure a level of security appropriate to the risk including the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

[Please note the inserted completion tips for, and instructions on, preparing confirmations of conformance with the agreed technical and organisational measures.]

These measures encompass the following:

1. Confidentiality (Article 32 (1) (b) GDPR)

- **[Admission] access control**

  Measures to prevent unauthorised persons from gaining access to data processing systems with which personal data are processed:

  [COMPLETION TIP to be deleted: To be completed by AGENT AND CONFIRMED TO PRINCIPAL]

- **[Machine usage] access control**

  Measures to prevent data processing systems from being used without authorisation:

  [COMPLETION TIP to be deleted: To be completed by AGENT AND CONFIRMED TO PRINCIPAL]

- **[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 in the course of processing:

  [COMPLETION TIP to be deleted: To be completed by AGENT AND CONFIRMED TO PRINCIPAL]

- **Separation control**

  Measures to ensure that data collected for different purposes are processed separately:

[COMPLETION TIP to be deleted: To be completed by AGENT AND CONFIRMED TO PRINCIPAL]

- **Pseudonymisation (Article 32 (1) (a) GDPR, Article 25 (1) GDPR)**

  The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures:

  [COMPLETION TIP to be deleted: To be completed and CONFIRMED TO PRINCIPAL only if agreed upon between AGENT and PRINCIPAL – only applies in exceptional cases

2. **Integrity (Article 32 (1) (b) GDPR)**

- **Transmission control**

  Measures to ensure 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:

  [COMPLETION TIP to be deleted: To be completed by AGENT AND CONFIRMED TO PRINCIPAL]

- **Input control**

  Measures to ensure 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:

  [COMPLETION TIP to be deleted: To be completed by AGENT AND CONFIRMED TO PRINCIPAL]

3. **Availability and resilience (Article 32 (1) (b) and (c) GDPR)**

- **Availability checks and rapid recoverability**

  Measures to ensure that personal data are protected against destruction and loss:

  [COMPLETION TIP to be deleted: To be completed by AGENT AND CONFIRMED TO PRINCIPAL]

4. **Procedures for regular inspection, assessment and evaluation (Article 32 (1)(d) GDPR; Article 25 (1) GDPR)**

- **Data protection management**

  [COMPLETION TIP to be deleted: To be completed by AGENT AND CONFIRMED TO PRINCIPAL]

- **Data protection-friendly default settings (Article 25 (2) GDPR)**

- Deletions can be performed in the systems deployed for the processing (deletability).
- Only data which are necessary in accordance with PRINCIPAL's guidelines are processed

- **[COMPLETION TIP to be deleted: These two issues are to be confirmed by the AGENT, and where appropriate to be complemented with further measures as well as confirmed to PRINCIPAL]**

  Job control

  Measures to ensure that personal data processed on a commissioned basis are processed strictly in accordance with the instructions of PRINCIPAL:

  [COMPLETION TIP to be deleted: To be completed by AGENT AND CONFIRMED TO PRINCIPAL]

Completion Tips

for the Agreement on the Technical and Organisational Measures

Please state which concrete technical and organisational measures you have taken to assure data protection and data security and send us confirmation of this.

One measure for warranting confidentiality and integrity is, notably, the use of state-of-the-art ***encryption procedures****. In addition to this, example measures are set out below.*

The individual measures must be described and explained plausibly and comprehensibly.

The Agreement on the Technical and Organisational Measures is an element of the Data Protection ***Annex*** *(DuD-B).*

Example measures for Confidentiality (№ 1):

[Admission] access control

- Card-based, personalised access control systems with [admission] access permission for authorised personnel only
- Work instructions for handling [admission] access controls
- Policies for accompanying and identifying guests in the building
- Server rooms secured with combination locks (code is only known to members of the IT department and is regularly changed)
- Policies for granting [admission] access rights to the server rooms
- Servers in lockable server cabinets, keys deposited with the IT department
- Organisational work directive for issuing keys
- Storage of backup tapes in an access-protected safe
- Laptops locked in cupboards after the end of work
- Building locked after the end of work and secured with an alarm facility and security guard service with regular patrols
- Barred windows

[Machine usage] access control

- Administration of server systems only possible with a console password or by means of a password-protected, encrypted connection
- Data encryption
- Use of client systems only possible after the user has been authenticated by means of a password-protected network authentication
- Blocking of user account after three abortive sign-on attempts
- Automatic, password-protected screensaver and computer lock after 10 minutes
- Audit-compliant, binding procedure for resetting “forgotten” passwords
- Audit-compliant, binding procedure for granting permissions
- Unambiguous matching of user accounts with users, no anonymous collective accounts (e.g. “TRAINEE1”)
- Policy on the secure, proper handling of passwords / smartcards
- Automated standard routines for regularly updating protection software (e.g. virus scanners)

[Data] access control

- Data encryption
- Permissions mechanism with the possibility of precise differentiation at a field level
- Audit-compliant, binding procedure for granting permissions
- Audit-compliant, binding procedure for restoring data from a backup (restore by IT department upon request by project management / department management / executive management / board management)
- Separation of the authorisation of permissions (organisational) by the department management / executive management / board management and the granting of permissions (technical) by the IT department
- Network drives (shares) with access for authorised users or user groups only

Separation control

- The data of the PRINCIPAL and other clients are processed as far as possible by different members of staff of the AGENT
- A permissions concept exists which supports the separate processing of the PRINCIPAL's data from the data of other clients
- The permission mechanisms available in the employed systems enable a precise implementation of the guidelines of the permissions concept

Pseudonymisation

Measures for pseudonymisation will only be possible as well as agreed upon with PRINCIPAL in exceptional cases , e.g. for test implementation

Example measures for Integrity (№ 2):

Transmission control

- Transport of backup tapes in backup safe by company's own courier service
- Sending of personal data e.g. by means of encrypted e-mail
- Data encryption
- Line encryption

Input control

- Contractual arrangements which restrict working with PRINCIPAL's personal data exclusively to the AGENT's personnel who are working in connection with the contractual performances
- Registration of the users and time of each change in the user management system

Example measures for Availability and Resilience (№ 3):

- Full backup and recovery concept with daily backups and disaster-proof storage of the data media
- Proof of the secure and proper archiving in a physically protected archive and binding mechanisms for the persons to whom access permissions are granted
- Competent use of protection programmes (virus scanners, firewalls, encryption programmes, SPAM filters) and written concept of how these are to be deployed (virus protection concept etc.)
- Use of hard disk mirroring
- Use of an uninterruptible power supply

Example measures for Regular Inspection, Assessment and Evaluation (№ 4):

Data protection management

- The AGENT has appointed a corporate data protection officer and, through its data protection

organisation, provides for his appropriate and effective integration into the relevant operational processes
- Regular audits (external)
- Regular reviews by the internal audit function

Data protection-friendly default settings (Article 25 (2) GDPR)

- The stated aspects of deletion and data storage are statutorily prescribed and the expected minimum requirements here
- Other measures which have been implemented by the AGENT should also be stated

Job control

- The contract contains detailed information about the nature and scope of the commissioned processing and usage of the PRINCIPAL's personal data.
- The contract contains detailed information about the reserved purposes for which the PRINCIPAL's personal data may be used, and a prohibition for the AGENT to use the data for any purpose other than for that formulated in the written commission.
- At the PRINCIPAL's request, a competent person may be contractually nominated at the AGENT who is authorised to issue instructions to the AGENT in regard to the agreed commissioned processing.

Instructions for Preparing the Confirmation Regarding Observance of the Agreed Technical and Organisational Measures

Under Article 28 GDPR, PRINCIPAL must regularly assure himself of conformance with the agreed technical and organisational measures (TOM) that have been taken by AGENT and are set out in the Data Protection Annex (DuD-B) of the contract. Rather than conducting an audit on-site on AGENT's premises, PRINCIPAL currently fundamentally regards a confirmation of AGENT's compliance with the agreed measures as sufficient assurance.

AGENT must therefore furnish PRINCIPAL with an appropriate confirmation from which the conformance of the technical and organisational measures agreed between PRINCIPAL and AGENT, and which have been implemented at AGENT's company can be deduced. AGENT may realise this confirmation by means of an up-to-date attestation, reports or report excerpts prepared by impartial parties (e.g. certified public accountants, AGENT's audit function, data protection officer, IT security department, quality auditors), or an appropriate certification from an IT-security or data-protection audit (e.g. in accordance with BSI Grundschutz).

In this connection, AGENT must confirm to PRINCIPAL that his in-house organisation is arranged such that the special requirements needed for data protection are fulfilled. Moreover, meaningful statements must be made with respect to the necessary data-protection and data-security measures (Article 32 GDPR).

AGENT must additionally confirm to PRINCIPAL that:

- the data entrusted to him are used exclusively for rendering the contractually agreed performances and that they are processed in accordance with the instructions of PRINCIPAL
- for handling the entrusted data, only such personnel is deployed that has received instruction in, and been obligated to, handling personal data in a data protection-conformant manner (notably upholding data secrecy) pursuant to GDPR and other relevant data protection regulations
- only subprocessors are charged whom AGENT has meticulously selected with respect to their implemented technical and organisational measures, and for whom AGENT has assured himself of their compliance, both prior to commencement of the data processing and thereafter (unless otherwise agreed from case to case), once a year;
- for commissioning these subprocessors, AGENT has in each case received the consent of PRINCPAL;
- the contractual arrangements agreed between AGENT and his own subprocessors (cascading commissioning) are worded such that they correspond with the contractual arrangements (Data Protection and Data Security Regulations – DuD-B) agreed between PRINCIPAL and AGENT; this relates notably to the technical and organisational measures which must exhibit an equivalent level of protection;
- in connection with rendering the contractually agreed performances, AGENT does not deploy any subprocessors whose place of business is situated outside the states of the EU/EEA[1] (third state) or who have access to the entrusted data from a third state; this also includes the inspection and maintenance of automated procedures and data processing systems if, in doing so, access to the entrusted data cannot be ruled out;
- the procedures that AGENT uses to render the agreed performances undergo regular audits and / or inspections.

From the above confirmation, it must ultimately be evident:

- who conducted the audits or inspections at AGENT's company;

[1] Provided that the application of GDPR has been endorsed as binding in the signatory states of the EEA.

- when, and with which focal points, the last inspections were performed;
- what the results of the inspection were (raised objections; whether findings are to be / were resolved at short notice etc.)
- at which time intervals the agreed technical and organisational measures are inspected.

Unless not yet done, AGENT must disclose to PRINCIPAL the name of his company's current data protection officer, along with the relevant contact details.

AGENT must furnish PRINCIPAL unbidden with a confirmation of the above-mentioned scope:

- before service provision (data processing) commences and thereafter
- regularly, once a year (starting from the time of the initial service provision) unless otherwise individually agreed.