Annex: Data Protection

Data Protection and Data Security Regulations (DuD-B)

- In connection with Order Nº dated

- In connection with Contract Nº dated

between

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

("PRINCIPAL")

and
…
…
…

("AGENT"),

jointly "Contract Parties"

1. This Annex "Data Protection and Data Security Regulations" ("DuD-B") concretises the undertakings of the Contract Parties which are required in accordance with data protection law and ensure from the Contract. It is valid for all performances and activities which are connected with the Contract, and for which coworkers deployed by AGENT or subcontractors charged by AGENT with the written consent of PRINCIPAL process personal data of PRINCIPAL.

2. The mutual liability of the Contract Parties for damages arising in connection with Commissioned Processing is governed by the provisions of DuD-B. If DuD-B makes no such provisions, the statutory provisions (notably Article 82 (5) of the General Data Protection Regulation) shall apply.

3. 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.

4. If PRINCIPAL is an institution or if a performance-receiving company within the PRINCIPAL's group of companies is an institution within the meaning of Section 1 (1b) 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

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 Contract and / or its Annexes.

1. Purpose of commision

AGENT processes personal data under commission by PRINCIPAL.

☐ The purpose of the data-handling commission is the execution of the following tasks by AGENT:

or

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

2. Duration of assignment

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

or (notably, if the 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…

or

☐ The commission is awarded for an unlimited period of time and can be terminated by either Contract Party with a notice period of … 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	☐
☐	☐

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:

4. Nature of the data

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

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

5. 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:

The persons authorised to receive instructions on behalf of AGENT are:

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:

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.

6. Consent to the commissioning of subcontractors

In no subcontractors are stated below, AGENT is prohibited from engaging one or more subcontractors.

AGENT may deploy the following subcontractor(s):

-

-

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

-

-

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

DuD-B is an integral part of the 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, for the rightfulness of the data processing within the meaning of Article 4 (2) GDPR, notably for the forwarding of data to AGENT and for exercising the rights of the data subjects. In doing so, AGENT shall support PRINCIPAL in an expedient manner. 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) When email communication is used, the Contract Parties shall uphold confidentiality by protecting confidential information from unauthorised disclosure and manipulation. For this purpose, the Contract Parties can agree on suitable technical measures such as, but not limited to, encryption and signature procedures.

(4) AGENT is aware that a violation of statutory data protection regulations can constitute a misdemeanour and possibly even a criminal act.

(5) AGENT confirms that he is familiar with the pertinent statutory data protection guidelines and that PRINCIPAL and AGENT, and possibly also any of their representatives, will cooperate in the event of inquiries which the supervisory authorities might conduct in the course of executing their duties.

(6) AGENT confirms and shall assure that persons charged with executing the commission have been obligated in writing to uphold confidentiality, and that they have been instructed in the data protection regulations of GDPR. The same undertaking applies for other data protection regulations (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)) to the extent that these are pertinent for the commission concerned. Upon PRINCIPAL's request, AGENT shall evince said undertaking and instruction.

(7) 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.

(8) If AGENT renders his services on the premises of PRINCIPAL or by means of accessing PRINCIPAL's systems, he shall be subject to the control facilities of PRINCIPAL (notably [Admission] access controls, [machine usage] access controls and [data] access controls).

(9) For the execution of the commission, AGENT undertakes, in accordance with the effective statutory data-protection regulations, to appoint in writing a Data Protection Officer. AGENT shall inform PRINCIPAL of the name of the Data Protection Officer. AGENT shall inform PRINCIPAL forthwith of any change in the office of Data Protection Officer. If AGENT is not required to appoint a Data Protection Officer in accordance with the effective statutory data protection guidelines, he shall take other suitable measures to ensure fulfilment of the duties required under the effective statutory data-protection guidelines.

(10) AGENT will regularly review the internal processes and technical and organisational measures to ensure that the processing in his realm of responsibility is conformant with

the requirements of effective data protection legislation and that the protection of the rights of the data subjects is warranted.

(11) AGENT shall support PRINCIPAL in observing GDPR with respect to the security of personal data, the notification obligation for data breaches, possibly in conducting data protection impact assessments and prior consultations and, notably, in upholding the rights of the data subjects pursuant to Articles 12 – 23 GDPR.

(12) AGENT may only issue information of a statutory data protection nature to third parties or to the data subjects subject to the prior written consent of PRINCIPAL.

(13) AGENT and possibly his representatives and subcontractors shall maintain a register of processing activities pursuant to Article 30 GDPR on all categories of processing activities which AGENT performs under commission by PRINCIPAL.

(14) AGENT shall, upon request, furnish PRINCIPAL with content from his register of processing activities which is of relevance for this Contract.

(15) 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.

(16) Amendments, supplements and collateral agreements, as well as unilaterally pronounced declarations of intent, such as, but not limited to, directives, confirmations or consents, must be made in writing pursuant to Section 126 of the German Civil Code (Bürgerliches Gesetzbuch, BGB). This applies additionally to amendments to the clause regarding the necessity for written form.

(17) AGENT processes personal data under commission by PRINCIPAL. This encompasses activities which are concretised in the Main Contract and in this Annex.

Section 2 – Data processing location

(1) The data will be processed exclusively within the territory of the Federal Republic of Germany, within a Member State of the European Union or within another signatory state of the European Economic Area (EEA) Treaty. If application of GDPR has not been endorsed as binding in the Member States of the EEA, the Member States of the EEA shall be deemed third states.

(2) Data processing in third states is prohibited. This also applies to subcontractors, 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 only occur if the special conditions of Article 44 et seq GDPR are satisfied.

(4) The processing of data off the operating premises of AGENT (e.g. from home offices, via teleworking or by means of remote access) is prohibited.

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 written directives of PRINCIPAL in doing so.

(2) Copies and / or duplicates 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.

(3) AGENT shall confirm verbally communicated work directives forthwith in writing. PRINCIPAL and AGENT will keep the written confirmation of the verbally communicated work directives in such way that all significant regulations are available at all times.

(4) 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 breach

(1) AGENT shall inform PRINCIPAL of, and identify remedies for, irregularities in the data processing workflow, founded suspicions of violations of guidelines and contractual agreements regarding 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, an audit or in any other data protection audit reports ("Data Protection Infringement") 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 forthwith and, whenever possible, within 24 hours of AGENT becoming aware of the breach.

(3) AGENT shall document every Data Protection Infringement. The documentation and notification of a Data Protection Infringement will contain at least the following information:

1. a description of the nature of the personal data protection breach and, where possible, details of the categories and approximate number of data subjects, the affected categories 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 personal data protection breach;
4. a description of the measures which AGENT has taken, or proposes be taken, to rectify the personal data protection breach and, possibly also, measures for mitigating the potentially detrimental impact thereof.

Moreover, AGENT shall furnish PRINCIPAL with all other information 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.

(5) AGENT shall compensate PRINCIPAL for all damages arising from a Data Protection Infringement, notably the cost of informing the data subjects and any administrative fine due to violation of the obligatory disclosure requirement pursuant to Articles 33 – 34 GDPR if culpable actions of AGENT were causal thereto.

Section 5 – Subcontractors

(1) The deployment of subcontractors by AGENT and / or further subcontractors (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 subcontractor. PRINCIPAL further reserves the right to issue his consent only if AGENT has demonstrated that his choice of subcontractor was made diligently after careful consideration of the suitability of the technical and organisational measures taken by the subcontractor.

(3) AGENT must contractually ensure that the regulations agreed between PRINCIPAL and AGENT also apply vis-à-vis subcontractors. Notably, PRINCIPAL must have the right to

conduct on-site checks of the subcontractor's premises, or to arrange for such checks to be conducted by a third party. AGENT must regularly verify fulfilment of the obligations.

(4) The contractual arrangements to be agreed between AGENT and the subcontractor 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 subcontractor must, notably, exhibit an equivalent level of security; the rights to issue instructions and the inspection rights must be preserved without restriction and the data processing must continue to be conducted in the EU / EEA.

(5) Upon PRINCIPAL's request, AGENT shall furnish information about the central content of the contract with the subcontractor and the implementation of the data protection-relevant obligations, if necessary by permitting inspection of the relevant contractual documents.

(6) If AGENT avails himself of a subcontractor 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 subcontractor, respectively the confirmations of the subcontractor's conformance.

(7) AGENT's scope of responsibility for the fulfilment of the activities he assigns to the subcontractor shall be the same as if AGENT had performed the activities himself. If the cascaded commissioned processor fails to fulfil his data protection obligations, the first commissioned processor shall be held liable vis-à-vis the Controller for fulfilment of the obligations of every other commissioned processor.

Section 6 – Correction, restriction, erasure and return of data

(1) AGENT may not without authorisation, but only with documented directives of PRINCIPAL, correct, erase 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 correction, erasure, blocking (in the context of imposing a restriction on processing pursuant to Article 4 № 3 GDPR) and surrendering of personal data, also at any time during, or after expiry of, the contractual period,.

(3) 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 contractual work. The erasure shall be evinced by way of a suitable erasure log. 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. The erasure shall be confirmed to PRINCIPAL in writing upon request. All rights of retention on the part of AGENT are excluded.

(4) Should a data subject approach AGENT directly in this regard, AGENT shall refer the request to PRINCIPAL forthwith.

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

(1) AGENT will arrange his organisation such that it satisfies the special requirements for data protection. In doing so, measures must be taken which are, notably, appropriate for the nature of the personal data or categories of data to be protected.

(2) 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.
(3) AGENT shall observe the principles for processing personal data set out in Article 5 (1) and (2) GDPR and warrants to implement the contractually agreed and legally required data security measures pursuant to Articles 24, 28 and 32 GDPR to evince the conformance of the processing with GDPR.
(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. This is also applicable to testing purposes.
(8) AGENT may not use personal data of PRINCIPAL during the development of software, or the inspection and maintenance of automated procedures or data processing facilities of PRINCIPAL. For this purpose, fictitious test data or, subject to the express, written consent of PRINCIPAL, original data that have rendered anonymous may be used.
(9) To protect personal data against misuse and loss (data security), AGENT shall implement the technical and organisational measures upon which the Contract Parties have agreed pursuant to DuD-B, Part 3 – TOM.
(10) 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, "Agreement on the Definition of the Technical and Organisational Measures", 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) AGENT warrants the proper implementation of the technical and organisational measures (DuD-B, Part 3, "TOM"). AGENT shall regularly 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).
(3) The Confirmation of Compliance shall be presented / made available to PRINCIPAL by AGENT unbidden, prior to commencing the data processing and, unless otherwise agreed from case to case, thereafter, once a year. 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 information or 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.

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.

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:

- **[Machine usage] access control**

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

- **[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:

- **Separation control**

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

- **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:

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:

- **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:

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:

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

   - **Data protection management**

   - **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

   - **Job control**

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

, date , date

PRINCIPAL	AGENT

Completion Tips

for the Agreement on the Technical and Organisational Measures

COMPLETION TIPS FOR AGENT – DELETE PAGE BEFORE CONTRACTUAL EXECUTION!!!

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 directives 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)

COMPLETION TIPS FOR AGENT – DELETE PAGE BEFORE CONTRACTUAL EXECUTION!!!

[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 AGENT's request, a competent person may be contractually nominated at the PRINCIPAL who is authorised to issue instructions to the AGENT in regard to the agreed commissioned processing.

COMPLETION TIPS FOR AGENT – DELETE PAGE BEFORE CONTRACTUAL EXECUTION!!!

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 written confirmation of AGENT's compliance with the agreed measures as sufficient assurance.

AGENT must therefore furnish PRINCIPAL with an appropriate, written 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 in writing 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 subcontractors 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 subcontractors, AGENT has in each case received the written consent of PRINCPAL;
- the contractual arrangements agreed between AGENT and his own subcontractors (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 subcontractors 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.