Processing Agreement according to Art. 28 of the General Data Protection Regulation (GDPR)

Framework agreement, valid for all assignments

between

[Full company name Client]
[Address]
[Place]
(Data Controller, hereinafter "**Client**")

and

Interflex Datensysteme GmbH
Epplestraße 225 / Haus 3
D-70567 Stuttgart
(processor, hereinafter referred to as the "**Contractor**")

§ 1   Subject and duration of the Agreement

(1)   <u>Subject</u>

The Contractor offers systems for automated access control and time recording as well as Advance Workforce Management.

This Agreement applies to all existing agreements and any agreements concluded in the future between the parties concerning the provision of specific IT services in relation to these systems by the Contractor to the Client (hereinafter referred to as "**Service Agreement**" even in the case of several agreements).

(2)   <u>Duration, termination</u>

Unless otherwise agreed, this Agreement shall apply for as long as the Contractor processes personal data in the course of the performance of the Service Agreement.

Either party may terminate the Agreement at any time without notice if there is a serious infringement by either party of data protection provisions or the provisions of this Agreement. In particular, failure to comply with the obligations set out in this Agreement and derived from Art. 28 GDPR constitutes a serious infringement.

§ 2   Initial provisions as to the content this Agreement

<u>Nature and purpose of processing of personal data</u>

The purpose of the processing of personal data by the Contractor on behalf of the Client, the types of data processed and the categories of data subjects are further described in the Service Agreement and in **Annex 1 – Specification under data protection law**.

The agreed data processing currently takes place exclusively within the Federal Republic of Germany, in another member state of the European Union or in another state party to the Agreement on the European Economic Area. Any relocation to a third country at a later point requires the Client's approval and is subject to the special requirements of Articles 44 et seqq. GDPR. The appropriate level of

protection can be ensured by standard data protection clauses (Art. 46 para. 2 sub-para. c and sub-para. d GDPR), by approved rules of conduct (Art. 46 para. 2 sub-para. e in conjunction with Art. 40 GDPR), through an approved certification mechanism (Art. 46 para. 2 sub-para. f in conjunction with Art. 42 GDPR) or by other measures pursuant to Art. 46 para. 2 sub-para. a, para. 3, sub-para. a and sub-para. b GDPR.

§ 3   Authority of the Client to issue instructions

(1)   The Contractor shall process personal data exclusively for the purpose of providing services under the Service Agreement and in accordance with the documented instructions of the Client. This also applies to any transfer of personal data to a third country or international organisation, unless required by the law of the European Union or of a Member State to which the Contractor is subject, in which case the Contractor shall notify the Client of such a requirement prior to processing, unless the law in question prohibits such notification on grounds of a substantial public interest. Instructions are issued by virtue of the Service Agreement and the setting up and configuration of the service by the Client. Further instructions after conclusion of the Agreement must be in text form and the Client must confirm them in writing if the Contractor so requests.

(2)   If the Client issues further instructions beyond the scope of the Service Agreement, this requires the consent of the Contractor.

(3)   If the Contractor is of the opinion that an instruction issued by the Client violates statutory provisions, the Contractor shall point this out to the Client. The execution of such an instruction may be suspended by the Contractor.

§ 4   Technical and organisational measures

(1)   Before starting processing, the Contractor shall document and submit to the Client for inspection the implementation envisaged for the technical and organisational measures stipulated prior to the award of the contract, in particular with regard to the concrete execution of the assignment. If accepted by the Client, these measures shall become the basis of the Agreement. Where the examination or an audit of the Client reveals a need for adjustment, this must be implemented by mutual agreement.

(2)   The Contractor shall ensure security of processing in accordance with Art. 28 para. 3 sub-para. c and Art. 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 GDPR. Generally speaking, the measures to be taken relate to data security and to ensuring a level of protection appropriate to the risk in terms of the confidentiality, integrity, availability and resilience of the systems. In this context, the state of the art, the implementation costs and the type, scope and purposes of processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR, must be taken into account (details in Annex 2 of this Agreement).

(3)   The technical and organisational measures taken are subject to technical progress and further development. In this respect, the Contractor may implement alternative adequate measures, provided that the security level of the initially stipulated measures is not undercut. Significant changes shall be documented in writing or electronically.

(4)   To the extent the Contractor performs its activity on-site at the Client, the Contractors is not responsible for the technical and organisational measures that are in the sphere of influence and responsibility of the Client.

§ 5 Quality assurance and other obligations of the Contractor

In addition to complying with the provisions of this Agreement, the Contractor has statutory obligations under Articles 28 to 33 GDPR. In this respect, the Contractor ensures compliance with the following requirements in particular:

a) Appointment in writing of a data protection officer pursuant to Articles 38 and 39 GDPR. This person can be reached at interflex.datenschutz@allegion.com.

   The current contact details of the data protection officer shall be easily available on the Contractor's website at all times.

b) Ensuring confidentiality pursuant to Art. 28 para. 3 p. 2 sub-para. b and Art. 29, 32 para. 4 GDPR. In performing the work, the Contractor shall only employ staff who are bound to confidentiality and who have previously been made aware of the provisions on data protection relevant to them.

c) Implementation of and compliance with all technical and organisational measures required for this Agreement in accordance with Art. 28 para. 3 p. 2 sub-para. c and Art. 32 GDPR (details in Annex 2 of this Agreement).

d) Upon request, the Client and the Contractor shall cooperate with the supervisory authority in the performance of its duties.

e) Immediate notification of the Client about measures and monitoring actions of the supervisory authority, insofar as they relate to this Agreement. This shall also apply where a competent authority, in the course of administrative or criminal proceedings relating to the processing of personal data, investigates processing activities at the Contractor.

f) Where the Client is himself subject to measures by the supervisory authority, to administrative or criminal proceedings, to a liability claim of a data subject or third party or to any other claim relating to the processing of personal data at the Contractor, the Contractor shall assist the Client to the best of his ability.

g) The Contractor shall regularly monitor internal processes implemented and technical and organisational measures taken to ensure that processing within his sphere of responsibility is carried out in accordance with applicable data protection law and that the rights of the data subjects are protected.

h) At the request of the Client, the Contractor shall provide the Client with evidence of the technical and organisational measures taken within the scope of the Client's supervisory powers under Article 7 of this Agreement.

i) Upon termination of the services to be provided under the Service Agreement or at the request of the Client, the Contractor shall return to the Client all documents in his possession and all work results and data produced in connection with the Agreement or erase them in accordance with data protection law with the prior consent of the Client.

j) The Contractor shall retain documentation that serves as evidence of proper data processing in accordance with the applicable retention periods beyond the end of the Agreement. The Contractor may hand over this documentation to the data controller upon termination of the Agreement.

§ 6   Subcontracting relationships

(1)   For the purposes of this provision, subcontracting relationships are deemed to relate directly to the provision of the main service. Subcontracted ancillary services, which do not primarily concern personal data processing, e.g. services around post, telecommunication, logistics, cleaning and skilled trades, are not included. However, even in the case of subcontracted ancillary services, the Contractor shall ensure the protection and security of the Client's personal data by means of adequate and legally compliant agreements and supervisory measures.

(2)   The Contractor may appoint an external processor (hereinafter referred to as the Subcontractor). By signing this Agreement, the Client gives the Contractor general permission to employ a Subcontractor. The Contractor shall inform the Client of any intended change regarding the use of Subcontractors, including their replacement. The Client may voice objections in relation to a Subcontractor and, if these are not resolved amicably, may terminate this Agreement as of the date on which the change takes effect. Currently, no subcontractors are engaged, unless such are listed in Appendix 3 - Subcontractors.

(3)   The Contractor shall, as a minimum and in compliance with applicable data protection law, transfer to Subcontractors the relevant obligations under this Agreement by way of (sub-)processing agreements, including appropriate technical and organisational measures to be taken.

(4)   The Contractor shall conclude confidentiality agreements with all Subcontractors, unless an adequate statutory confidentiality obligation applies.

§ 7   Supervisory powers

(1)   The Client may, at his own expense, before the start of data processing and thereafter at regular intervals, satisfy himself of the technical and organisational measures taken by the Contractor pursuant to Annex 2 and document the results. This can be done, *inter alia*, by obtaining a self-disclosure from the Contractor, which the Contractor can also provide in the form of a suitable certificate from an expert or by the Client conducting an on-site inspection.

(2)   The Contractor undertakes to provide the Client, upon written request and within a reasonable period of time, with all information necessary in the context of an appropriate inspection.

(3)   If the Client commissions a third party to carry out an inspection (including an on-site inspection), the Client shall oblige this third party in writing to maintain secrecy and confidentiality, unless the third party is subject to a professional obligation of secrecy. At the request of the Contractor, the Client shall submit the corresponding agreements with the third party to the Contractor without delay. The Client may not commission any of the Contractor's competitors with an inspection.

(4)   Any on-site inspection requires a written advance notice of 30 days, as a general rule, and is limited to ordinary business hours and has to be undertaken in a way so it minimizes any impact of the Contractor's business operations. Any routine on-site inspections are limited to a maximum of 1 time per calendar year. The Client shall share in writing the result of its inspection within (as a general rule) 30 days from the completion of the inspection.

§ 8   Rights of the data subjects

(1)   The rights of persons affected by the processing of personal data shall be asserted against the client.

(2)   Where a data subject contacts the Contractor directly for information on, or rectification, erasure or blocking of, data concerning him or her, the Contractor shall forward this request to the Client without undue delay.

(3)   In the event that a data subject asserts his or her data protection rights, the Contractor shall, within reasonable limits and to the extent necessary for the Client, support the Client with suitable technical and organisational measures, provided that the Client cannot handle a given claim without the Contractor's cooperation.

(4)   The Contractor shall enable the Client to rectify, erase or block personal data or, at the Client's request, rectify, block or erase such data himself if and to the extent that this cannot be done by the Client.

§ 9   Notification in the event of infringements by the Contractor

(1)   The Contractor shall assist the Client in complying with the obligations set out in Articles 32 to 36 GDPR on the security of personal data, reporting in the event of data breaches, data protection impact assessments and prior consultations. This includes *inter alia*:

   a) ensuring an adequate level of protection by technical and organisational measures which take into account the circumstances and purposes of data processing as well as the predicted likelihood and severity of potential infringements caused by security breaches and which are designed to enable immediate detection of relevant infringements;
   b) the obligation to assist the Client in his duty to provide information to data subjects, making all relevant information available to the Client without delay;
   c) supporting the Client with data protection impact assessments, as required;
   d) assisting the Client in the course of prior consultations with the supervisory authority.

(2)   The Contractor is aware that the Client may be subject to a notification obligation pursuant to Art. 33 GDPR, which requires notification to the supervisory authority within 72 hours of a circumstance becoming known. The Contractor shall support the Client with any such notification obligation.

(3)   The Contractor shall inform the Client without undue delay if he becomes aware of a personal data breach in the course of data processing.

(4)   Where the Client becomes subject to statutory notification obligations regarding unlawful acquisition of personal data as the result of an incident, the Contractor shall assist the Client in meeting these obligations at the Client's request within the scope of what is reasonable and necessary. Such assistance shall be subject to remuneration unless the incident has been culpably caused by the Contractor or it is part of the service description of the Service Agreement.

§ 10   Rectification, erasure and restriction of data processed

(1)   The Contractor may not rectify, erase or restrict the data processed under this Agreement on his own authority, but only following documented instructions from the Client. Where a data subject contacts the Contractor directly in this respect, the Contractor shall forward this request to the Client without delay.

(2)   Data which the Contractor merely processes for the performance of the services (e.g. maintenance) shall be erased as soon as they are no longer needed for the respective service (cf. Annex 2 – Access control).

§ 11   Liability

Art. 82 GDPR applies. Where the Service Agreement contains provisions on liability, these shall also apply to the relationship between the parties within the scope of this Agreement.

§ 12   Obligation to pay remuneration

(1)   Where the Contractor is obliged by this Agreement to provide services beyond the scope of the Service Agreement ("**Additional Services**"), these services shall be remunerated separately according to time and material expended. This is particularly the case for the activities set out in 3 (2), Art. 5 sub-para. d and sub-para. f, Art. 7 (excepting services needed due to a breach within the Contractor's responsibility), Art. 8 and Art. 10. For the avoidance of doubt, to the extent that the Contractor has culpably caused any Additional Services, the Client does not owe a remuneration under this §12.

§ 2   (2) Subject to the Service Agreement or any other agreements between the parties, the remuneration for Additional Services of the Contractor's employees is based on an hourly flat rate of EUR 180 plus statutory value added tax. For material and travel expenses, the Contractor shall invoice the Client in the amount actually incurred plus value added tax. Should the Contractor be able to prove additional costs, he may invoice the full amount.

§ 13   Miscellaneous

(1)   Supplements and amendments to this Agreement must be made in writing. This also applies to any waiver of the written form requirement.

(2)   Should any provision of this Agreement prove legally invalid, the validity of the remaining provisions shall remain untouched. The invalid provision shall be replaced retroactively by a provision that is as close as possible to the original provision in terms of content and business effect.

(3)   This Agreement is governed by German law (under exclusion of international private law). Exclusive place of jurisdiction for any and all disputes arising from and in connection with this Agreement is Stuttgart, Germany.

Interflex Datensysteme GmbH   **Name of Client**

_____   _____
Signature   Signature

_____   _____
Name, function   Name, function

_____   _____
Date, stamp   Date, stamp

Annex 1 – Specification under data protection law

This Annex 1 (Specification under data protection law) complements the respective Service Agreement concluded. It goes without saying that only the personal data that are part of the agreed scope of services will be processed.

Categories of data subjects:
1. Employees within the meaning of Art. 26 para. 8 of the German Federal Data Protection Act (BDSG-neu), who use the IF system
2. Visitors/external workers, if necessary with visitor/guest badge for the IF system, if the corresponding module is covered by the Service Agreement.

Data types per service components:
The following types of data (defined in detail below), if part of the processing assignment, may be processed by the Contractor:

	Services of the Contractor associated with processing (Art. 28 GDPR)				
	Commissioning and repair of the booking terminals	**Commissioning of the software**	**Software upgrades and updates for Interflex IF System(s)**	**Software maintenance in the form of troubleshooting**	**Data processing via secure remote access (e.g. VPN connection)**
Products/Systems					
IF 6020 *The Interflex System IF-6020 is a modular software application. In most applications, terminals for time recording and/or access control are connected.*	- Booking data, access - Booking data, time recording	- Personal master data - Booking data, access - Booking data, time recording including web client - Workflow data, access control - Workflow data, time recording - Frontend data - Payroll accounts - Badge creation data - Visitor/third party data	- Personal master data - Booking data, access - Booking data, time recording including web client - Workflow data, access control - Workflow data, time recording - Frontend data - Payroll accounts - Badge creation data - Visitor/third party data	- Personal master data - Booking data, access - Booking data, time recording including web client - Workflow data, access control - Workflow data, time recording - Frontend data - Payroll accounts - Badge creation data - Visitor/third party data - Workforce planning and management data	- Personal master data - Booking data, access - Booking data, time recording including web client - Workflow data, access control - Workflow data, time recording - Frontend data - Payroll accounts - Badge creation data - Visitor/third party data - Workforce planning and management data
Products/Systems					
IF 6040	- Booking data, access	- Personal master data	- Personal master data	- Personal master data	- Personal master data

The Interflex System IF-6040 is a modular software application. In most applications, terminals for time recording and/or access control are connected.	- Booking data, time recording	- Booking data, access - Booking data, time recording including web client - Workflow data, access control - Workflow data, time recording - Frontend data - Payroll accounts - Badge creation data - Visitor/third party data	- Booking data, access - Booking data, time recording including web client - Workflow data, access control - Workflow data, time recording - Frontend data - Payroll accounts - Badge creation data - Visitor/third party data	- Booking data, access - Booking data, time recording including web client - Workflow data, access control - Workflow data, time recording - Frontend data - Payroll accounts - Badge creation data - Visitor/third party data - Workforce planning and management data	- Booking data, access - Booking data, time recording including web client - Workflow data, access control - Workflow data, time recording - Frontend data - Payroll accounts - Badge creation data - Visitor/third party data - Workforce planning and management data
SP-EXPERT *The Interflex System SP-EXPERT is a modular software application.* *In most applications, workforce planning and management data are generated or used.*	- Booking data, access - Booking details Time recording	- Personal master data - Variable data - Time management data - Booking data, time recording - Frontend data - Payroll accounts	No IF system	- Personal master data - Variable data - Time management data - Booking data, time recording - Frontend data - Payroll accounts - Workforce planning and management data - Log files - Transfer directories with data imported from or exported to other systems	- Personal master data - Variable data - Time management data - Booking data, time recording - Frontend data - Payroll accounts - Workforce planning and management data - Log files - Transfer directories with data imported from or exported to other systems
Badge customisation	Badge creation data	Badge creation data	Badge creation data	Badge creation data	Badge creation data
Visitor/third party customisation	Visitor/third party data	Visitor/third party data	Visitor/third party data	Visitor/third party data	Visitor/third party data

Definition of the data types:

Booking data, access	Access bookings with booking terminal, time stamp and result of the authorisation check.	**Payroll accounts**	Hourly totals for the payroll system
Personal master data	Master record number, badge number, surname, first name, personnel number, department and optional fields, if used by the Client within the system	**Frontend data**	Data transfer/data exchange with wage and salary system. Data records consisting of: Master record number, badge number, surname, first name, personnel number, department, time recording booking data and optional fields, if used by the Client within the system. Data communication depends on the configuration (customising) of the interface.
Booking data, time recording including web client	Time recording booking type with booking terminal, time stamp and balances of the time accounts; reasons for absence (off-site work, business trip, sick leave, training, holiday, etc.); absences (from to); absenteeism totals (hours per day) – options/permissibility of 'reason for absence' entries and notifications are determined by the Client.	**Badge creation data**	Customisation data for the visible imprint on the badge medium (surname, first name, signature, and possibly digital photo). These data and possibly date of signature can be stored in the module for the creation of the badge.
Workflow data, access control	Requests for access authorisations; approver and acknowledgement approved yes/no; e-mail address used for workflow communication	**Visitor/third party data**	Registration data, if necessary for the visible imprint on the badge medium/pass (surname, first name, possibly signature and, if necessary, digital photo). Length of stay, pre-registration data, person being visited, reason for visit, individual visitors, permanent visitors.
Workflow data, time recording	Requests for corrections, reasons for absence, absences; approver and acknowledgement approved yes/no; e-mail address for workflow communication	**Workforce planning and management data**	Functions, qualifications, time availability, shift schedules/work centre planning, statistical data from the ACD (telephone system) for preparing personnel requirements, time account evaluations.

Annex 2 - Technical and organisational measures

1. Confidentiality (Article 32 para. 1 sub-para. b GDPR)

- Access control (physical)
  No unauthorised access to data processing facilities, whereby the concept is to be understood spatially.

  Technical/organisational measures for access control, in particular for the legitimation of authorised persons:

  ⇨ Access control system with badge readers for chip cards

  ⇨ Keys/key allocation

  ⇨ Door protection (electric door openers, etc.)

  ⇨ Reception for visitors

  Access to the buildings/parts of buildings at Interflex is via electronic IF access control. Visitors/external companies can only enter the Interflex building parts after registration and approval. They are accompanied by the person being visited.

- Access control (logical)

  The intrusion of unauthorised persons into the data processing systems must be prevented.

  Technical (password protection) and organisational (user master record) measures regarding user identification and authentication:

  ⇨ Controlled password procedure (syntax at least 1 special character or 1 capital letter, 1 digit, lower case, minimum length = 10, regular password change every 90 days, repeat cycle = 24)

  ⇨ Automatic blocking (e.g. password or pause circuit)

  ⇨ Setting up a user master record per user and function

  ⇨ Encryption of data media with AES 256 Bit Zip program or VeraCrypt or similar programs.

  ⇨ Encryption/Tunnel connection (VPN = Virtual Private Network)

  All the Contractor's computer systems have a user name and an individual password. If required, they are connected to the intranet manually using Active Directory. External access to the intranet is only possible via VPN. Access is only granted if the identification data of the computer, user name and password are known there and match. The syntax of the passwords, which must be changed at regular intervals, is at least 10 characters, special characters or capital letters, lower case and at least one digit. The repeat cycle is 24. These conditions are automatically checked when the password is changed, and if they are not met, the new password is rejected. If a password is not changed in time, it expires and access is denied.

- Access right control

  Unauthorised activities in data processing systems beyond the scope of the authorisations granted must be prevented.

  Demand-based design of the authorisation concept and access rights as well as their monitoring and logging:

  ⇨ Differentiated authorisations and temporary password assignment (according to the Interflex System authorisation concept) by the Client

⇨ Storage of data provided on a local computer in encrypted containers (e.g. using VeraCrypt or similar programs). The local computer itself must be completely encrypted using an enterprise solution.

⇨ Access limited to the person carrying out the respective data processing

Data provided to the Contractor is stored for the duration of processing in local, encrypted containers (e.g. VeraCrypt or similar programs) and is removed after completion of the work using a special eraser. The local data media on computers are additionally completely encrypted using an enterprise solution. Temporary data storage is limited to the local systems of those commissioned to carry out the assignment. Only authorised Interflex users have access to the PC.

Access control to the data of the Interflex Client system is regulated by the Client himself by assigning/specifying/deleting a temporary password.

- Data separation

Data collected for different purposes must be processed separately.

Measures for separate processing (storage, modification, erasure, transmission) of data with different purposes:

⇨ "Internal multi-client capability"/earmarking

⇨ Separation of functions/production/test

Client data is stored and processed temporarily in encrypted, password-protected containers, while being kept strictly separate from other Client data. In the case of processing via online remote control, changes are made directly in the Client's system. There is a separate server for test data.

- Pseudonymisation (Art. 32 para. 1 sub-para. a GDPR; Art. 25 para. 1 GDPR)
The processing of personal data in such a way that the data cannot be related to a specific data subject without the provision of additional information, provided that this additional information is kept separately and is subject to appropriate technical and organisational measures.

For the purposes of service, data provided by the Client are usually handled in a pseudonymised form. If required, the data can be anonymised. The exact procedure depends on the particular service case.

2. Integrity (Article 32, par. 1 sub-para. b GDPR)

- Transfer control

Handling aspects of the transfer of personal data: Electronic transmission, data transport, transmission control. No unauthorised reading, copying, modification or removal.

Measures during transport, transfer and transmission or storage on data media (manual or electronic) and subsequent verification:

⇨ Encryption/tunnel connection (VPN = Virtual Private Network)

⇨ Data backups using a Zip program (e.g. WinZip) and 256-bit AES encryption using a password on CD/DVD

⇨ Logging

As a rule, the data is not passed on, except where solving a problem requires the cooperation of the Contractor's development department. Should this become necessary, the data backup is either transferred on a CD/DVD sent by post, using a Zip program, 256-bit AES encryption

and a password, or, for small amounts of data, directly via the Intranet using a Zip program and 256-bit AES encryption. Any such transfer is documented appropriately.

- Input control

  Measures of data management and maintenance must be documented for traceability.

  Measures for subsequent verification whether and by whom data have been entered, changed or removed (erased):

  ⇨ Logging via log file in Interflex system(s).

    The IF systems have a log file in which the changes are entered with the respective user ID as well as date and time.

3. Availability and resilience (Art. 32 para. 1 sub-para. b GDPR)

- Availability control

  The data must be protected against accidental destruction or loss.

  Measures for data backup (physical/logical):

  ⇨ No backup procedure for Client data backups because of data protection-compliant deletion after the purpose has ceased to apply

  ⇨ Virus protection / Firewall

  ⇨ UPS for Servers

  Data backups of Client systems are not backed up on servers with a backup function, so that the erasure of this data in accordance with data protection regulations can be ensured after the purpose has ceased to apply.
  All computer systems are checked for viruses after each startup using Microsoft System Center Endpoint Protection. The anti-virus files are updated every time the computer starts up in the company network. An automatic full check is performed weekly.

- Rapid recoverability (Art. 32 para. 1 sub-para. c GDPR);

  a) There are several servers for the Contractor's own systems. Data protection through daily backups. Virtualisation of the systems with centralised backup in preparation
  b) Client systems:
     Where data is transmitted to Interflex, this is not original data but merely copies of data and/or databases. No backup is made so as to ensure erasure after the purpose of pro-cessing has ceased to exist, i.e. after the assignment has been completed. The original data will remain in the Client's system. Responsibility for the data in the Client's system lies with the Client.

4. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 sub-para. d GDPR; Art. 25 para. 1 GDPR)

- Data protection management;
- incident response management: Is included in the ISMS (information security management sys-tem)
- Data protection by default (Art. 25 para. 2 GDPR);
- Continuous monitoring
- Restores of backups for test purposes
- Regular tests of the UPS
- Assignment control

No data processing within the meaning of Art. 28 GDPR without corresponding instructions from the Client

Measures (technical/organisational) for delimiting responsibilities between the Client and the Contractor:

⇨ Unambiguous drafting of contracts in accordance with Art. 28 GDPR

⇨ Formalised placing of orders (maintenance contract or written individual assignments)

The Contractor shall carry out the commissioned scope of services by his own means, without Subcontractors, in accordance with the Client's instructions.
As a matter of principle, commissioned changes are made to the programs and the evaluation logic only.

Annex 3 - Subcontractors

1. ⊠ Currently no subcontractors are employed.

2. ☐ Currently the following subcontractors are engaged:

Company name subcontractor	Address/Country	Service