Data Processing Agreement (DPA)

Framework agreement, valid for all assignments

between

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

and

Allegion International AG
Interflex
Mellingerstrasse 207 / Täfernhof
5405 Baden-Dättwil
Switzerland
(Processor, hereinafter referred to as the "**Contractor**")

§ 1 Subject matter and duration of this DPA

(1) Subject

The Contractor offers systems for automated access control, visitor management and time recording as well as workforce management.

This DPA 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).

The systems of the Contractor are typically operated as on-premises solutions at the Client and by the Client, however, it cannot be excluded that - in the context of the above-mentioned specific IT services - the Contractor is granted access to personal data in accordance with and subject to this DPA.

(2) Duration, termination

This DPA shall apply for as long as the Contractor processes personal data in the course of the performance of the Service Agreement unless otherwise agreed.

Either party may terminate the Service Agreement at any time without notice if there is a serious infringement by the other party of data protection provisions or the provisions of this DPA. In particular, failure to comply with the obligations set out in this DPA and derived from Art. 9 Swiss Federal Act on Data Protection (FADP) respectively 28 GDPR (to the extent applicable) constitutes a serious breach.

§ 2 Initial provisions as to the content of this DPA

Nature and Purpose of the intended processing of personal data

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 in the territory of the Federal Republic of Germany, in another member state of the European Union or of 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 Art. 16 FADP respectively 44 et seqq. GDPR (to the extent applicable).

§ 3 Authority of the Client to issue instructions

(1) The Contractor shall process the 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 Service 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) The Client may name to the Contractor, in text form by an authorized person, the persons authorized to issue instructions - or any change of persons authorized to issue instructions - for the execution of the processing under this DPA. In principle, the responsible key account manager or project manager or service technician are the recipients of instructions in the case of the Contractor, unless a person authorized to represent the Contractor has informed the Client otherwise in text form.

§ 4 Technical and organisational measures (TOM)

(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 this DPA. 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. 9 and 8 FADP respectively Art. 28 para. 3 sub-para. c and Art. 32 GDPR (to the extent applicable), in particular in conjunction with Art. 6 FADP respectively Art. 5 para. 1, para. 2 GDPR (to the extent applicable). 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 nature, 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. 8 FADP respectively Art. 32 para. 1 GDPR (to the extent applicable), shall be taken into account (details in Annex 2 of this DPA).

(3) The technical and organisational measures taken are subject to technical progress and further development. In this respect, the Contractor is permitted 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 Contractor is not responsible for the technical and organisational measures that are in the sphere of influence and/or in the responsibility of the Client.

(5) To the extent the Contractor performs services at the Customer's premises, the Contractor shall not be responsible for compliance with the technical and organizational measures that lie within the Customer's sphere of influence and responsibility.

§ 5 Quality assurance and other obligations of the Contractor

In addition to complying with the provisions of this DPA, the Contractor has statutory obligations under Art. 9 FADP respectively Art. 28 to 33 GDPR (to the extent applicable). In this respect, the Contractor ensures compliance with the following requirements in particular:

a) Appointment in writing of a data protection officer pursuant to Art. 10 FADP respectively Art. 38 and 39 GDPR (to the extent applicable).

   The current contact details of the data protection officer are available on the Contractor’s website at all times.

b) Ensuring confidentiality pursuant to Art. 8 FADP respectively Art. 28 para. 3 p. 2 sub-para. b and Art. 29, 32 para. 4 GDPR (to the extent applicable). 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 DPA in accordance with Art. 10 FADP respectively Art. 28 para. 3 p. 2 sub-para. c and Art. 32 GDPR (details in Annex 2 of this DPA).

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 DPA. 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 § 7 of this DPA.

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 Service 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 Service Agreement. The Contractor may hand over this documentation to the Client upon termination of the Agreement.

§ 6 Subcontracting relationships

(1) For the purposes of this DPA, 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 craftsman services, 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 DPA, 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 DPA 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 DPA 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 of the Client

(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 thirty (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) thirty (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 Rectification, erasure and restriction of data processed

(1) The Contractor may not rectify, erase or restrict the data processed under this DPA 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).

§ 10 Notification in the event of infringements

(1) The Contractor shall assist the Client in complying with the obligations set out in Art. 8 FADP respectively Art. 32 to 36 GDPR (to the extent applicable) 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. 24 FADP respectively Art. 33 GDPR (to the extent applicable), which requires notification to the supervisory authority as soon as reasonably possible, however, in any case 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.

(5) If the Client uses an on-premise solution operated by the Client himself, the contractor's obligation to support in accordance with this § 10 only exists to the extent it is not possible for the Client to obtain the required information himself or cannot carry out the required activities himself.

§ 11 Liability

The customary rules on liability of Swiss Code of Obligations apply. Additionally, Art. 82 GDPR may apply. Where the Service Agreement contains provisions on liability, these shall also apply to the relationship between the parties within the scope of this DPA.

§ 12 Compensation obligation

Where the Contractor is obliged by this DPA 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), § 5 lit. d) and lit. f), § 7 (excepting services needed due to a breach within the Contractor's responsibility), § 8, § 9 and § 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. For Additional Services the agreed rates as per the Service Agreement (or otherwise agreed) shall apply.

§ 13 Miscellaneous

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

(2) Should any provision of this DPA 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) The right to plead the right of retention shall hereby be excluded with regard to the data processed for the Client.

(4) Should the Client's data be jeopardised by the Contractor by seizure, by insolvency proceedings or by other events or measures taken by third parties, the Contractor shall inform the Client immediately. The Contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lie exclusively with the Client as the controller within the meaning of FADP respectively GDPR (to the extent applicable).

(5) This DPA is governed by Swiss law (under exclusion of international private law). Exclusive place of jurisdiction for any and all disputes arising from and in connection with this DPA is the seat of the Processor.

[signature page to follow]

Allegion International AG	**Name of Client**
Signature	Signature
Name, function	Name, function
Date	Date

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 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. 8 FADP respectively 28 GDPR, as applicable)				
	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.
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
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.
Workflow data, access control	Requests for access authorisations; approver and acknowledgement approved yes/no; e-mail address used for workflow communication
Workflow data, time recording	Requests for corrections, reasons for absence, absences; approver and acknowledgement approved yes/no; e-mail address for workflow communication

Payroll accounts	Hourly totals for the payroll 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.
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.
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.
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. 1. Confidentiality

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

  Technical/organizational measures for access control, in particular for the legitimation of authorized persons:

  ⇨ Access control systems 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 unauthorized persons into the data processing systems must be prevented.

  Technical (password protection) and organizational (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 use and function

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

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

  For login to Contractor's computer systems each employee uses an individual username and password (respectively admin credentials for administrators). 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, username and password are known there and match. The syntax of the passwords, which must be changed in 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 authorization concept and access rights as well as their monitoring and logging:

⇨ Differentiated authorizations and temporary password assignment (according to the Interflex System authorization 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.

Within the contractor's systems, authorizations are granted exclusively on a need-to-know basis. Extraordinary authorizations are subject to a documented approval workflow.

A process for granting authorizations is in place, which, among other things, also changes the assignment of rights and authorizations in the event of changes (e.g., department changes) or departures.

Users are not granted administrator rights per se. If necessary, local admin rights can be requested, stating the reasons, and undergo an approval workflow. If approved, administrator activities are logged.

- 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.

- Pseudonymization
  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 organizational measures.

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

2. Integrity

- Transfer control

  Handling aspects of the transfer of personal data: Electronic transmission, data transport, transmission control. No unauthorized 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 or similar programs) and 256-bit AES encryption with password

⇨ 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

  The data must be protected against accidental destruction or loss.

  Measures for subsequent verification of whether and by whom data has been entered, changed or removed (deleted):

  ⇨ 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

- 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 in order to confirm with data protection requirement to delete after the purpose has ceased to apply

  ⇨ Virus Protection / Firewall / Patch-Management

  ⇨ UPS for servers

  ⇨ Regular maintenance of IT hardware or use of leased equipment

  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 equipped with anti-virus programs. after each startup using Microsoft System Center Endpoint Protection. The antivirus signatures are updated promptly after they are released via the centrally controlled Endpoint Protection solution. An automatic full check is performed weekly. All servers are protected against power fluctuations or power failure by means of a UPS.

- Rapid recoverability;

  a) There are several servers for the Contractor's own systems. Data protection through daily backups. Virtualization of the systems with centralized 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 processing 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.

- Resilience:

  a) The utilization of the Interflex's own systems, such as servers, networks, and internet systems, is monitored with real-time incident-reporting.
  b) Data recovery is also possible across multiple locations thanks to the backup concept. Live testing of the systems is in operation, which includes vulnerability assessment and automated reporting.
  c) Regularly reviewed emergency and recovery plans are in place to ensure rapid response in the event of system failures.

4. Procedures for regular review, assessment and evaluation

- Data Protection Management;
- Incident Response Management: Is included in the ISMS (information security management system)
- Data protection by default;
- Continuous monitoring
- Restores of backups for test purposes
- Regular tests of the UPS
- Patch-Management
- Change-Management
- Mandatory awareness trainings for all employees

- Assignment control
  No data processing without corresponding instructions from the Client

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

  ⇨ Unambiguous drafting of contracts

  ⇨ Formalized placing of orders (maintenance contract or written individual assignments

  The Contractor shall carry out the commissioned scope of services in principle by his own means or by Subcontractors, as the case may be, 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**
Interflex Datensysteme GmbH	Epplestr. 225, 70567 Stuttgart, Germany	Hersteller, zusätzlicher Support (z.B. 2nd und 3rd Level)