Data Processing Agreement (DPA) in accordance with Art. 28 of the General Data Protection Regulation (GDPR)

for Interflex Cloud Services

between

the Client
- as identified in more detail in the Interflex Cloud Services contract -
(Responsible person, hereinafter the "**Client**")

and

Interflex Datensysteme GmbH
Epplestraße 225
70567 Stuttgart
(Processor, hereinafter the "**Contractor**")

§ 1 Subject matter and duration of this DPA

(1) Subject

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

This data processing agreement (DPA) applies to all processing of personal data pursuant to the Interflex Cloud Services Contract (hereinafter "**Service Agreement**"). This DPA is attached to the Interflex Cloud Services Contract as Annex 3.

(2) Duration, termination

The Agreement 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 DPA at any time without notice if a serious breach of a party against data protection regulations or the provisions of this DPA. In particular, non-compliance with the obligations agreed in this DPA and derived from Art. 28 GDPR constitutes a serious breach.

§ 2 Concretization of the content of the DPA

purpose of the intended processing of personal data

The purpose of the processing of personal data by the Contractor for the Client, the types of data processed and the categories of data subjects are described in more detail in the Service Agreement and in **Annex 1 - Data Protection Legal Specification.**

The provision of the contractually agreed data processing currently takes place exclusively in the territory of the Federal Republic of Germany, in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. A possible later relocation to a third country requires the consent of the Client and must fulfil the special requirements of Art. 44 et seq. GDPR.

§ 3 Authority of the Client to issue instructions

(1) The Contractor shall process the personal data exclusively for the provision of its services under the Service Agreement in accordance with the Client's documented instructions, including with regard to the transfer of personal data to a third country or an international organisation, unless it is obliged to do so by the law of the Union or of a Member State to which it is subject; in such a case, the Contractor shall notify the Client of these legal requirements prior to the processing, unless the law in question prohibits such notification due to an important public interest. The instructions shall otherwise result from the Service Agreement and the setting and configuration of the service carried out by the Client. Individual instructions after the conclusion of the agreement must be in text form and the Client must confirm them in writing if requested by the Contractor.

(2) If the Client issues individual instructions that go beyond the scope of services agreed in the Service Agreement, this shall require the Contractor's consent.

(3) The Contractor shall draw the Client's attention to the fact if, in its opinion, an instruction issued by the Client violates statutory provisions. The Contractor shall be entitled to suspend the implementation of the relevant instruction.

(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 Agreement. 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-organisational measures

(1) The Contractor shall document the implementation of the agreed technical and organisational measures before the start of the processing, in particular with regard to the specific execution of the Service Agreement, and shall hand them over to the Client for inspection. If accepted by the Client, the documented measures shall become the basis of this DPA. Insofar as an examination/audit of the Client reveals a need for adaptation, this shall be implemented by mutual agreement.

(2) The Contractor shall establish the security of the processing pursuant to Art. 28 (3) lit. c, 32 GDPR, in particular in connection with Art. 5 (1), (2) GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR shall be taken into account (details in Annex 2, which is an integral part of this DPA).

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

(4) Insofar as the Contractor performs services on the Client's premises, the Contractor shall not be responsible for compliance with the technical and organisational measures which are within the Client's sphere of influence and responsibility.

§ 5 Quality assurance and other obligations of the Contractor

In addition to compliance with the provisions of this commissioned processing, the Contractor shall have legal obligations pursuant to Art. 28 to 33 of the GDPR; in this respect, the Contractor shall in particular ensure compliance with the following requirements:

a) Written appointment of a data protection officer pursuant to Art. 38 and 39 of the GDPR.

   The current contact details of the data protection officer(s) are always available on the Contractor's homepage.

b) Maintaining confidentiality in accordance with Art. 28 (3) sentence 2 lit. b, 29, 32 (4) GDPR. When carrying out the work, the Contractor shall only use employees who have been obligated to maintain confidentiality and who have previously been familiarised with the data protection provisions relevant to them.

c) The implementation of and compliance with all technical and organisational measures required for this commissioned processing pursuant to Art. 28 (3) sentence 2 lit. c, 32 GDPR (details in Annex 2, which is part of this DPA).

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

e) The immediate information of the Client about control actions and measures of the supervisory authority, insofar as they relate to this commissioned processing. This shall also apply to the extent that a competent authority investigates the Contractor in the context of administrative offence or criminal proceedings with regard to the processing of personal data in the course of the processing under this DPA.

f) Insofar as the Client, for its part, is exposed to an inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with the commissioned processing at the Contractor, the Contractor shall support it to the best of its ability.

g) The Contractor shall regularly monitor the internal processes as well as the technical and organisational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.

h) Upon request by the Client, the Contractor shall provide evidence of the technical and organisational measures taken to the Client within the scope of its control powers pursuant to § 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, in accordance with the Service Agreement, all documents in its possession and all work results and data created in connection with the Agreement or delete them in accordance with data protection law with the prior consent of the Client.

j) The Contractor shall retain documentation that serves as proof of proper data processing in accordance with the applicable retention periods beyond the end of the Agreement. The Contractor may hand over the documentation to the Client at the end of this DPA.

§ 6 Subcontracting relationships

(1) Subcontracting relationships within the meaning of this DPA are those services which relate directly to the provision of the main service. This does not include ancillary services where the subcontracting does not primarily concern the processing of personal data, e.g. the use of postal, telecommunications, logistics, cleaning and craftsman services. However, the Contractor shall be obliged to implement appropriate and legally compliant contractual agreements as well as control measures to ensure data protection and data security of the Client's personal data also in the case of outsourced ancillary services.

(2) The Contractor may appoint an external processor (hereinafter referred to as a "**Subcontractor**"). By signing this DPA, the Client gives the Contractor general permission to employ Subcontractors. The Contractor shall inform the Client of any intended change with regard to the engagement or replacement of Subcontractors. The Client may notify any objections to the Subcontractor and, if these are not resolved by mutual agreement, terminate this DPA as of the date on which the change takes effect. No Subcontractors are currently used unless such Subcontractors are listed in **Annex 3 - Subcontractors**.

(3) The Contractor shall at least pass on the obligations under this DPA to its Subcontractors within the framework of (sub)commissioned processing agreements to be concluded, including the guarantee of appropriate technical and organisational measures. These must comply with the requirements of the applicable data protection law.

(4) The Contractor shall enter into confidentiality agreements with all Subcontractors insofar as they are not already subject to a corresponding statutory confidentiality obligation.

§ 7 Control rights of the Client

(1) The Client may, at its own expense, convince itself of the technical and organisational measures taken by the Contractor in accordance with Annex 2 prior to the commencement of data processing and regularly thereafter and document the result. This can be done, among other things, by obtaining a self-disclosure from the Contractor, which the Contractor can also fulfil by submitting a suitable certificate from an expert, or by carrying out 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 required to carry out a corresponding inspection.

(3) If the Client commissions a third party to carry out the inspection (including an on-site inspection), the Client shall oblige the third party in writing to maintain secrecy and confidentiality, unless the third party is subject to a professional confidentiality obligation. At the request of the Contractor, the Client shall submit the obligation agreements with the third party to the Contractor without delay. The Client may not commission a competitor of the Contractor with the 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. Routine on-site inspections shall be limited to a maximum of once per calendar year. The Client shall inform the Contractor in writing of the result of its inspection, as a general rule within thirty (30) days of completion of the inspection.

§ 8 Rights of the data subjects

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

(2) Insofar as a data subject should contact the Contractor directly for the purpose of information, correction, deletion or blocking of the data concerning him, the Contractor shall forward this request to the Client without delay.

(3) In the event that a data subject asserts its rights under data protection law, the Contractor shall support the Client with suitable technical and organisational measures in the fulfilment of these claims to the extent appropriate and necessary for the Client, provided that the Client cannot fulfil the claims without the Contractor's cooperation.

(4) The Contractor shall enable the Client to correct, delete or block personal data or, at the Client's request, carry out the correction, blocking or deletion itself if and to the extent that this is impossible for the Client itself.

§ 9 Notification in the event of infringements

(1) The Contractor shall assist the Client in complying with the personal data security obligations, data breach notification obligations, data protection impact assessments and prior consultations referred to in Articles 32 to 36 of the GDPR. This includes, among others

a) Ensuring an adequate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a potential security breach and allow for the immediate detection of relevant breach events
b) the obligation to assist the Client within the scope of its duty to inform the data subject and, in this context, to provide it with all relevant information without delay
c) the support of the Client for its data protection impact assessment, as far as necessary
d) the support of the Client within the framework 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 of the GDPR, which provides for notification to the supervisory authority within 72 hours of becoming aware of the matter. The Contractor shall support the Client in the corresponding reporting obligations.

(3) The Contractor shall inform the Client without delay if it becomes aware of a personal data breach within the scope of the commissioned processing.

(4) Insofar as the Client is subject to statutory duties to provide information due to unlawful acquisition of personal data, the Contractor shall support the Client in fulfilling the duties to provide information at the Client's request within the scope of what is reasonable and necessary. The cooperation is subject to remuneration, unless it is included in the service description or the violation is due to the fault of the Contractor.

§ 10 Correction, restriction and deletion of data

(1) The Contractor may not correct, delete or restrict the processing of data processed under this DPA on its own authority, but only in accordance with documented instructions from the Client. Insofar as a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without delay.

(2) Data that the Contractor processes only for the performance of its services (e.g. maintenance) are deleted as soon as they are no longer required for the provision of the respective service (cf. Annex 2 (Access Control).

§ 11 Liability

Art. 82 GDPR shall apply. Insofar as the Service Agreement contains provisions on liability, these shall also apply to the internal relationship of the parties within the scope of this DPA.

§ 12 Compensation obligation

Insofar as the Contractor is obliged by this DPA to perform services which are not included in the scope of services according to the Service Agreement ("**Additional Services**"), these shall be remunerated separately according to time and material expenditure. This is in particular the case for the services described in § 3(2), § 5 lit. d) and f), § 7 (insofar as services are not required due to a data protection breach for which the Contractor is responsible), § 8 and § 10 activities mentioned above. The Parties clarify that, insofar as the Contractor should have unlawfully caused Additional Services, the Client shall not owe any remuneration pursuant to this § 12. For Additional Services the agreed rates as per the Service Agreement (or otherwise agreed) shall apply.

§ 13 Miscellaneous

(1) Additions 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 be legally invalid, this shall not affect the validity of the remaining provisions. The ineffective provisions shall be replaced retroactively by a provision that is as close as possible in terms of content to the economic purpose of the intended provision.

(3) The defence of the right of retention within the meaning of section 273 BGB (German Civil Code) shall be excluded with regard to the data processed for the Client and the associated data carriers.

(4) Should the Client's data at the Contractor be endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Client thereof without delay. The Contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Client as the person responsible within the meaning of the GDPR.

(5) This DPA shall be governed by German law to the exclusion of the application of private international law. The exclusive place of jurisdiction for all disputes arising from and in connection with this DPA is Stuttgart, Germany.

Annex 1 - Data protection specification: Interflex Cloud Services:

This Annex 1 (Data Protection Specification) must be read together with the concluded Service Agreement (Interflex Cloud Services Contract). It goes without saying that only the personal data that are part of the agreed scope of services will be processed.

Categories of persons concerned:

1. Employees who use the IF system
2. Visitors/external workers, if applicable with visitor/guest pass for the IF system, if corresponding module agreed in the Service Agreement.

Data types:
The following types of data may be processed by the Contractor, insofar as they are part of the commissioned service:

Badge creation data	Personalisation data for the visible imprint on the ID medium (surname, first name, signature if applicable and digital photo if applicable). This data and, if applicable, the date of signature can be stored in the module for the creation of the ID card.
Visitor external company data	Registration data, if applicable for the visible imprint on the identification medium/pass (surname, first name, signature if applicable and digital photo of the person concerned if applicable). Length of stay, pre-registration data, person visited, reason for visit, individual visitor, permanent visitor.
Booking data Time recording including web client	Booking type Time recording with booking terminal, time stamps and balances of the time accounts; missing reasons (business trip, business trip, sick, seminar, holiday, etc.); absences (from to); absence totals (hours per day) - The Client determines the possibilities/admissibility of the missing reason entries and missing reason displays.
Booking data access	Booking type Access with booking terminal, time stamp and result of the authorisation check.
Login data	Login data
Payroll accounts	Hourly totals for the salary/settlement system
Staff planning and control data	Functions, qualifications, time availability, shift schedules/workplace planning, statistical data from the ACD (telephone system) for preparing staffing requirements, time account evaluations.
Personal master data	Master record number, badge number, surname, first name, personnel number, department and the optional fields, if these are used by the Client in the system.
Pre-calculator data	Data transfer/ data exchange with payroll system. Data records consisting of: Master record number, badge number, surname, first name, personnel number, department, booking data time recording and the optional fields, if these are used by the Client in

	the system. Data communication depends on the respective configuration (customising) of the interface.
Workflow data Access control	Applications for access authorisations; approver and feedback approved yes/no; e-mail address official for workflow communication.
Workflow data Time recording	Requests for corrections, reasons for errors, absences; approver and feedback approved yes/no; e-mail address official for workflow communication.

Annex 2 - Technical-organisational measures

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

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

  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 (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 system)
- Data protection by default (Art. 25 para. 2 GDPR);
- 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 within the meaning of Art. 28 GDPR without corresponding instructions from the Client

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

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

  ⇨ 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 Subcontracting relationships

a) ☐ Subcontracting does not currently take place.

b) ☒ The following subcontracting relationships exist as of the date of this DPA:

Company Subcontractor	**Address/Country**	**Power**
IONOS SE	Elgendorfer Str. 57, 56410 Montabaur, Germany	Operator Data Centres and Computer Platforms (IaaS)