Intrexx

# *Agreement on Order Processing*

Status: June 2025

## 1. General information

1.1. The Contractor processes personal data on behalf of the Client within the meaning of Art. 4 (8) and Art. 28 of Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR). This Contract governs the rights and obligations of the parties in connection with the processing of personal data.

1.2. Insofar as the term "data processing" or "processing" (of data) is used in this Contract, the definition of "processing" within the meaning of Art. 4 (2) GDPR shall apply.

## 2. Subject matter of the Contract

2.1. The subject matter in terms of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects is set out in **Annex 1** to this Contract.

## 3. Rights and obligations on the part of the Client

3.1. The Client is the controller within the meaning of Art. 4 (7) GDPR for the processing of data on behalf of the Contractor. Pursuant to Section 4 (2), the Contractor has the right to inform the Client if, in its opinion, legally unauthorised data processing constitutes the subject of the order and/or an instruction.

3.2. As the controller, the Client is responsible for safeguarding the rights of the data subjects. The Contractor shall inform the Client immediately if data subjects assert their rights as data subjects against the Contractor.

3.3. The Client has the right to issue supplementary instructions to the Contractor at any time regarding the data processing type, scope and procedure. Instructions must be issued in text form (e.g. email).

3.4. This shall be without prejudice to any provisions regarding compensation for additional expenses incurred by the Contractor as a result of additional instructions issued by the Client.

3.5. The Client may appoint persons authorised to issue instructions. If persons authorised to issue instructions are to be appointed, they shall be identified in **Annex 1** . In the event that the persons authorised to issue instructions on behalf of the Client change, the Client shall inform the Contractor of this in text form.

3.6. The Client shall inform the Contractor immediately if it discovers errors or irregularities in connection with the processing of personal data by the Contractor.

3.7. In the event that there is an obligation to inform third parties pursuant to Art. 33, 34 GDPR or any other statutory reporting obligation applicable to the Client, the Client shall be responsible for ensuring compliance with this obligation.

## 4. Obligations on the part of the Contractor

4.1. The Contractor shall process personal data exclusively within the framework of the agreements made and/or in compliance with any supplementary instructions issued by the Client. Exceptions to this are legal regulations that may oblige the contractor to process the data in another way. In any such case, the Contractor shall notify the Client of these legal requirements prior to processing, unless the law in question prohibits such notification due to a substantial public interest. The purpose, type and scope of data processing shall otherwise be governed exclusively by this Contract and/or the instructions issued by the client. The Contractor is prohibited from processing data in any other way unless the Client has consented to this in writing.

4.2. Generally speaking, the Contractor shall carry out data processing on behalf of the Client in member states of the European Union (EU) or the European Economic Area (EEA). The Contractor is also permitted to process data outside the EU or EEA if appropriate subcontractors are used in the third country, in compliance with the requirements of Section 9 and provided the requirements of Art. 44-48 GDPR are met or an exception within the meaning of Art. 49 GDPR exists.

4.3. The Contractor shall inform the Client immediately if, in its opinion, an instruction issued by the Client violates legal regulations. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Client. If the Contractor can demonstrate that processing in accordance with the Client's instructions may result in liability on the part of the Contractor under Art. 82 GDPR, the Contractor shall be entitled to suspend further processing in this respect until the liability has been clarified between the parties.

4.4. The Contractor may designate to the Client the person(s) authorised to receive instructions from the Client. If persons authorised to receive instructions are to be appointed, they shall be identified in **Annex 1.** In the event that the persons authorised to receive instructions on behalf of the Contractor change, the Contractor shall inform the Client of this in text form.

4.5. The Contractor shall support the Client in its obligation to respond to requests to exercise data subject rights in accordance with Art. 12-23 GDPR. The provisions of Section 11 of this Contract shall apply.

4.6. The Contractor shall support the Client in complying with the obligations set out in Art. 32-36 GDPR, taking into account the type of processing and the information available to it.

## 5. Contractor's appointed data protection officer

5.1. The Contractor confirms that it has appointed a data protection officer in accordance with Art. 37 GDPR. The Contractor shall ensure that the data protection officer has the necessary qualifications and expertise. Upon request, the Contractor shall inform the Client separately in text form of the name and contact details of its data protection officer.

5.2. The obligation to appoint a data protection officer in accordance with paragraph 1 may be waived at the discretion of the Client if the Contractor can prove that it is not legally obliged to appoint a data protection officer and the Contractor can prove that operational regulations exist that guarantee the processing of personal data in compliance with statutory provisions, the provisions of this contract and any further instructions issued by the Client.

## 6. Reporting obligations on the part of the Contractor

6.1. The Contractor is obliged to notify the Client immediately of any breach of data protection regulations or of the contractual agreements concluded and/or the instructions issued by the Client that has occurred during the course of the processing of data by the Contractor or other persons involved in the processing. The same shall apply to any breach of the protection of personal data processed by the Contractor on behalf of the Client.

6.2. Furthermore, the Contractor shall inform the Client immediately if a supervisory authority takes action against the Contractor pursuant to Art. 58 GDPR and this may also entail a check of the processing that the Contractor performs on behalf of the Client.

6.3. The Contractor is aware that the Client may be subject to a reporting obligation pursuant to Art. 33, 34 GDPR, which prescribes that the supervisory authority be notified within 72 hours of a situation coming to light. The Contractor shall support the Client in implementing the reporting obligations. In particular, the Contractor shall notify the Client of any unauthorised access to personal data processed on behalf of the Client immediately upon becoming aware of such access. The Contractor's notification to the Client must include the following information in particular:

6.4. A description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, the categories concerned and the approximate number of personal data records concerned;

6.5. A description of the measures taken or proposed to be taken by the Contractor to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.

## 7. Regulations regarding mobile workplaces

7.1. The Contractor may authorise its employees who are commissioned to process personal data for the Client to process personal data at mobile workstations outside the Contractor's business premises.

7.2. The Contractor shall ensure that compliance with the contractually agreed technical and organisational measures is also guaranteed in instances where the Contractor's employees use mobile workstations. Deviations from individual contractually agreed technical and organisational measures must be agreed with the Client in advance and approved by the Client in text form.

7.3. In particular, the Contractor shall ensure that, when processing personal data at mobile workstations, the storage locations are configured in such a way that the local storage of data on IT systems is excluded. If this is not possible, the Contractor shall ensure that local storage is exclusively encrypted and that other persons at the location of the respective mobile workstation do not have access to this data.

7.4. The contractor is obliged to ensure that effective monitoring of the processing of personal data on behalf of the client at mobile workstations is possible.

7.5. If employees are also to be deployed at mobile workstations by subcontractors, the provisions of paragraphs 1 to 4 shall apply accordingly.

## 8. Monitoring authority

8.1. The Client shall have the right to monitor the Contractor’s compliance with the statutory provisions on data protection and/or compliance with the contractual provisions agreed between the Parties and/or compliance with the Client's instructions to the extent necessary.

8.2. The Contractor shall be obliged to provide the Client with information insofar as this is necessary to perform monitoring within the meaning of paragraph 1.

8.3. The Client may carry out monitoring within the meaning of paragraph 1 at the Contractor's premises during normal business hours after prior notification with reasonable notice. The Client shall ensure that monitoring is only carried out to the extent necessary so as not to disproportionately disrupt the Contractor's business operations as a result of the inspections. The parties assume that an inspection will be required no more than once a year. Further inspections must be justified by the Client, stating the reason. In the event of on-site inspections, the Client shall reimburse the Contractor for any expenses incurred, including personnel costs for the supervision and support of the

inspectors on site, within a reasonable scope. The Contractor shall inform the Client of the basis for the cost calculation before the inspection is carried out.

8.4. At the Contractor's discretion, proof of compliance with the technical and organisational measures may also be provided in place of an on-site inspection by means of the submission of a suitable, current certificate, reports or report extracts from independent bodies (e.g. auditors, internal audit, data protection officer, IT security department, data protection auditors or quality auditors) or a suitable certification, if the audit report enables the Client to be reasonably assured of compliance with the technical and organisational measures in accordance with Annex 3 to this Contract. If the client has reasonable doubts concerning the suitability of the test document within the meaning of sentence 1, an on-site inspection may be carried out by the Client. The Client is aware that on-site inspections in data centres are not possible or are only possible in justified exceptional cases.

8.5. The Parties agree that the monitoring measures concerning the processing of personal data at mobile workstations with a view to protecting the personal rights of other persons at these mobile workstations shall primarily be carried out by checking that the measures to be taken by the Contractor in accordance with Section 8 (2) and (3) are ensured. The Contractor must also afford the Client the opportunity to monitor the mobile workstations of employees on an ad hoc basis.

## 9. Subcontracting relationships

9.1. The Contractor is authorised to use the subcontractors specified in **Annex 2** to this Contract for the processing of data on behalf of the Client. The changing of subcontractors or the commissioning of further subcontractors is permitted under the conditions specified in paragraph 2.

9.2. In the event of a planned change of subcontractor or the planned commissioning of a new subcontractor, the Contractor shall notify the Client in text form in good time, but no later than 3 weeks prior to the change or new commissioning ("Notification"). The Client shall have the right to object to the change or new commissioning of the subcontractor in text form within three weeks of receipt of the "Information", stating the reasons. The objection may be withdrawn by the Client in text form at any time. In the event of an objection, the Contractor may terminate the contractual relationship with the Client with a notice period of at least 14 days to the end of a calendar month. The Contractor shall give reasonable consideration to the Client’s interests when giving notice of cancellation. If no objection is made by the Client within three weeks of "Notification", this shall be deemed to constitute the Client's granting of consent to the change or reassignment of the concerned subcontractor.

9.3. The Contractor must select the subcontractor carefully and ensure that it can fulfil the agreements made between the Client and the Contractor prior to commissioning. In particular, the Contractor must check in advance and regularly during the term of the

Contract that the subcontractor has taken the technical and organisational measures required under Art. 32 GDPR regarding the protection of personal data. The result of the check must be documented by the Contractor and forwarded to the Client on request.

9.4. If the Contractor places orders with subcontractors, the Contractor shall be responsible for transferring its data protection obligations under this Contract to the subcontractors and for concluding a contractual agreement with them in accordance with Art. 28 (2-4) GDPR. In particular, the Contractor guarantees that the subcontractor's TOMs meet the level of protection of the TOMs outlined in Annex 3 of this Agreement.

9.5. Services that the Contractor utilises, which are provided by third parties as a purely ancillary service with a view to carrying out the business activity are not to be regarded as subcontracting relationships within the meaning of paragraphs 1 to 4. These include, for example, cleaning services, pure telecommunication services with no specific connection to services that the Contractor provides for the Client, postal and courier services, transport services and security services. The Contractor is nevertheless obliged to ensure that appropriate precautions and technical and organisational measures have been taken to guarantee the protection of personal data, even in the case of ancillary services provided by third parties. The maintenance and servicing of IT systems or applications constitutes a subcontracting relationship requiring consent and order processing within the meaning of Art. 28 GDPR if the maintenance and testing relate to IT systems that are also used in connection with the provision of services for the Client and where personal data that is processed on behalf of the Client can be accessed during maintenance.

## 10. Confidentiality obligation

10.1. When processing data on behalf of the Client, the Contractor is obliged to maintain the confidentiality of data that it receives or of which it becomes aware in connection with the order.

10.2. The Contractor warrants that it is aware of the applicable data protection regulations and that it is familiar with their application. The Contractor further warrants that it has familiarised its employees with the data protection provisions applicable to them and has obliged them to maintain confidentiality. The Contractor further warrants that it has, in particular, obliged the employees involved in carrying out the work to maintain confidentiality and has informed them of the Client's instructions.

## 11. Safeguarding the rights of data subjects

11.1. The Client is solely responsible for safeguarding the rights of data subjects. The Contractor is obliged to support the Client in its obligation to process requests from data subjects in accordance with Art. 12-23 GDPR. In particular, the Contractor must ensure that the information required in this respect is provided to the Client without delay so that the Client can fulfil its obligations under Art. 12 (3) GDPR.

11.2. Insofar as the cooperation of the Contractor is necessary for the protection of data subject rights - in particular, rights to information, correction, blocking or deletion - by the Client, the Contractor shall take the necessary measures in each case in accordance with the Client's instructions. Where possible, the Contractor shall support the Client with suitable technical and organisational measures in order to fulfil its obligation to respond to requests to exercise data subject rights.

11.3. This shall be without prejudice to any provisions concerning compensation for additional expenses incurred by the Contractor as a result of cooperation services in connection with the assertion of data subject rights vis-à-vis the Client.

## 12. Confidentiality obligations

12.1. Both parties undertake to treat all information that they receive in connection with the execution of this Contract as confidential, for an unlimited period of time, and to use it exclusively for the execution of the Contract. Neither Party is authorised to use this information in whole or in part for purposes other than those just mentioned or to make this information accessible to third parties.

12.2. The above obligation does not apply to information that one of the parties has demonstrably received from third parties without being obliged to maintain confidentiality or that is publicly known.

## 13. Remuneration

Any provisions on remuneration for services shall be agreed separately between the Parties.

## 14. Technical and organisational data security measures

14.1. The Contractor undertakes vis-à-vis the Client to comply with the technical and organisational measures required to comply with the applicable data protection regulations. This includes, in particular, the requirements of Art. 32 GDPR.

14.2. The status of the technical and organisational measures existing at the time of the conclusion of the Contract is attached as **Annex 3** to this Contract. The Parties agree that changes to the technical and organisational measures may become necessary in order to adapt to technical and legal circumstances. The Contractor shall agree in advance with the Client any significant changes that may affect the integrity, confidentiality or availability of personal data. Measures that only entail minor technical or organisational changes and do not negatively affect the integrity, confidentiality and availability of personal data can be implemented by the Contractor without consultation with the Client. The Client may request an updated version of the technical and organisational measures taken by the Contractor once a year or on justified occasions.

## 15. Duration of the contract

15.1. The Contract shall commence upon signature and shall run for the duration of the main Contract existing between the Parties for the use of the Contractor's services or products by the Client.

15.2. The Client may terminate the Contract at any time without notice if there is a serious breach on the part of the Contractor of the applicable data protection regulations or of obligations under this Contract, if the Contractor is unable or unwilling to carry out an instruction from the Client or if the Contractor denies access to the Client or the competent supervisory authority in breach of the Contract.

## 16. Termination

16.1. Upon termination of the Contract, the Contractor shall, at the Client's discretion, return to the Client or delete all documents, data and processing or utilisation results that have come into its possession in connection with the contractual relationship. The deletion must be documented in a suitable manner. Any statutory retention obligations or other obligations to store the data shall remain unaffected.

16.2. The Contractor may store personal data that has been processed in connection with the order beyond the termination of the Contract if and to the extent that the Contractor has a legal obligation to store the data. In these cases, the data may only be processed for the purposes of implementing the respective statutory retention obligations. After expiry of the retention obligation, the data must be deleted immediately.

## 17. Rights of retention

The Parties agree that the defence of the right of retention by the Contractor within the meaning of § 273 BGB (German Civil Code) is excluded with regard to the processed data and the associated data carriers.

## 18. Final provisions

18.1. Should the Client's property held by the Contractor be jeopardised by third-party measures (such as seizure or confiscation), insolvency proceedings or other events, the Contractor must inform the Client immediately. The Contractor shall immediately inform the creditors of the fact that the data in question is being processed on behalf of the Client.

18.2. Additional agreements must be made in writing.

18.3. Should individual parts of this Contract be invalid, this shall not affect the validity of the remaining provisions of the contract.

18.4. All annexes mentioned in these terms and conditions are a binding part of the Contract.

# *Annex 1 - Object of the Contract*

## 1. Object and purpose of the processing

The Client's order placed with the Contractor generally comprises the following work and/or services. Further details on the subject matter and purpose of the processing of personal data can be found in the respective main Contract:

The Client uses the Contractor's software product, "Intrexx", which is provided as Software-as-a-Service (SaaS) or Platform-as-a-Service (PaaS). This is a low-code application platform software.

The Contractor provides maintenance services to the Client during the use of the SaaS or PaaS. These include the patch management of the Contract Software and the infrastructure used, the provision of secure access to the Contract Software (web-based), backup and recovery management.

The Contractor shall maintain the software and support the Client in its use. The Contractor shall make changes to the software settings as instructed by the Client.

## 2. Categories of data subject

The personal data relates to the end users of the platform and to persons whose personal data is provided by the end users of the platform. This includes, among others:

- Interested parties and/or customers of the client
- Employees of the client, including former employees
- Suppliers/service providers of the client

## 3. Type(s) of personal data

The personal data processed may include the following categories of data:

**On-Site / On-Premise:**

- Direct identifying information (e.g. name, email address, telephone number).
- Indirect identifying information (e.g. job title, gender, date of birth, user ID).
- Any personal data contained in a document provided by the customer.
- Special categories of personal data included in the platform by the customer.
- Ticket data

**SaaS / cloud platform:**

- Direct identifying information (e.g. name, email address, telephone number).
- Indirect identifying information (e.g. job title, gender, date of birth, user ID).
- Data for device identification and traffic data (e.g. IP addresses, MAC addresses, web protocols) and associated log data or usage history
- All personal data provided by the users of the cloud platform
- All personal data contained in a document provided by the customer

- Special categories of personal data included in the platform by the customer.
- Log, ticket and maintenance data

## 4. Contractor's persons authorised to receive instructions

- Markus Grauvogl, INTREXX GmbH (CEO)
  +49 761 20703 332, Markus.Grauvogl@intrexx.com

- Christoph Böttcher, INTREXX GmbH (Head of Risk & Compliance)
  +49 761 20703 390, Christoph.Boettcher@intrexx.com

## 5. Data Protection Officer

The Contractor has appointed a data protection officer:

Sven Bartsch, Secure Data GmbH +49 5966 9268795, Datenschutzbeauftragter@intrexx.com

The Client must be informed immediately of any change of data protection officer.

# *Annex 2 - Subcontractors*

For the processing of data on behalf of the Client, the Contractor utilises the services of third parties who process data on its behalf ("subcontractors").

These are the following companies:

| Subcontractor | Type of service |
|---|---|
| Continum AG<br>Bismarckallee 7b-d \| D-79098 Freiburg | Server hosting |
| Amazon Web Services EMEA<br>Sarl 38, avenue John F. Kennedy \| L-1855<br>Luxembourg | Server hosting |
| badenIT GmbH<br>Tullastr. 61 \| D-79108 Freiburg | Server hosting |
| Superluminar<br>Völckersstraße 14-20 \| 22765 Hamburg | Consultancy AWS |

# *Annex 3 - Technical and organisational measures*

## 1. Data protection and data security concept

The following measures describe the individual technical and organisational measures taken by INTREXX within the context of order processing in accordance with Art. 24 (1) GDPR.

The GDPR obliges companies to take appropriate technical and organisational measures to secure the processing of personal data and to anonymise or pseudonymise personal data wherever possible. The measures taken must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of data subjects, appropriate technical and organisational measures, so as to ensure a level of security appropriate to the risk.

INTREXX GmbH fulfils these requirements through an effective combination of data protection management and information security management. In addition, appropriate measures have been taken to safeguard data processing operations. In particular, this includes measures with regard to the following protection values: confidentiality, integrity, availability and resilience.

The protection values are based on the following definitions relevant to information security:

**Confidentiality:**
Information and related infrastructure may only be available to authorised persons.

**Integrity:**
Information may only be changed by authorised persons and only in the manner intended for that person. Integrity refers to the integrity of information with the aim of protecting it from unauthorised changes.

**Availability / recoverability:**
Information must be made accessible to authorised persons within the required timeframe and with the required quality, and must also be usable.

**Resilience:**
As a special aspect of availability, resilience requires that systems are designed to be as resilient as possible – even in the event of a malfunction, error or high load.

## 2. Confidentiality

Confidentiality within the meaning of Art. 32 (1) (b) GDPR includes technical and organisational measures that ensure that personal data is only accessible to a specific group of recipients. This includes physical access control, system access control, data access control and separation control as well as other measures such as anonymisation and pseudonymisation.

## 2.1 Physical access control

INTREXX GmbH has implemented technical and organisational measures to secure physical access control at its company headquarters. In addition, the servers of the data processing system are outsourced to an externally operated data centre. Only those persons whose presence is required to carry out or secure operations or to perform inspection tasks are authorised to physically access this data processing system.

The subcontractor for the housing is commissioned and is responsible for ensuring physical access control for the data centre.

The physical access controls are:

### 2.1.1 Data centre

2.1.1.1 Site and property security

- The data centre is located in its own secure area, in an external ISO/IEC27001 certified data centre
- Servers are located there in separate, locked cabinets
- Access to the badenIT data centres is controlled by means of physical access control systems (electronically coded key or code card with badge reader)
- Controlled key allocation and authorisation allocation by code card to a strictly limited group of people
- In both cases, access is logged
- Building security installations:
- Perimeter defence by means of cordoned-off premises
- Access via gatekeeper service
- Intruder alarm systems
- Use of the security service
- Video surveillance of the entrance area to the data centre
- 2.1.1.2 Access authorisation regulations
- Documented access regulations for authorised visitors
- Group of persons defined by Intrexx GmbH (IT personnel, management) for authorised access to the data processing systems of Intrexx GmbH
- Authorised persons must identify themselves to gain access
- Every access instance is logged
- Security zones and restrictive access authorisations, the group of (system) administrators is limited to the minimum required size and is documented

**2**.1.2 Company headquarters

- There are no data-processing server systems at the company headquarters.
- Access to the building is controlled by means of an access control system
- Access to the office space of Intrexx GmbH is only granted to authorised persons. These are employees of Intrexx GmbH and the contracted cleaning company
- Access is only granted to third parties when accompanied and is logged
- Security zones for technical areas are in place and limited to a minimum number of authorised employees by means of restrictive access authorisations
- Controlled transponder allocation incl. documentation

## 2.2 System access control

System access control involves documenting all technical and organisational measures that are suitable for preventing the use of data processing systems, usually computers, by unauthorised persons.

### 2.2.1 General regulations on access authorisations

- Access to the IT systems of INTREXX GmbH is only possible after authentication using a user name and password;
- Documented allocation of user accounts;
- Administrator accounts are only used for strictly limited activities;
- Logged, verifiable use of access to data processing systems;
- Passwords are subject to a password policy in which requirements such as length, complexity, retention period, reuse of previously used passwords, etc. are defined.
- Passwords of administrators are subject to higher requirements;
- Disconnection or blocking of the connection in the event of repeated failed attempts or timeouts where possible;
- Rules established for cases of loss or compromise of passwords;
- Critical systems are equipped with 2-factor authentication;
- Awareness-raising and obligation of employees to lock the computer when leaving the workstation so that a password entry is required to unlock it. An automatic screen lock is also configured;
- Separate network infrastructure for visitors and employees
- Rules for deactivating unused accounts;
- Network access is blocked; in general, no external systems are authorised in the internal INTREXX GmbH network;
- Securing of the network infrastructure through intrusion detection systems, use of two-factor authentication where possible, separation of networks, content filters, encrypted network protocols;

### 2.2.2 Additional measures in case of remote access

- Documentation of persons who are authorised to log in externally;
- Network access security through hardware and software measures;
- Unauthorised access from the Internet is prevented by means of the use of firewalls;
- Strong authentication using e.g. token and PIN;
- Logging of remote access at the (SSL) VPN gateway.
- Remote access restricted to a minimum of network access for service providers/freelancers in accordance with the work order

## 2.3 Data access control

It must be ensured that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data is not read, copied, modified or removed without authorisation during processing, use and after storage.

### 2.3.1 Authorisation concept

- Documented and traceable processes for obtaining, changing, managing and revoking access authorisations;
- Access authorisations and user groups are managed in a central directory service as far as possible;
- Individual access authorisations are assigned at individual or group level;
- Authorisations require an upstream approval process.

### 2.3.2 Access protection

- Use of encryption routines and the option of file encryption;
- Regulations for the encryption of mobile devices;
- Measures in place to secure network access; only authorised hardware and software used;
- Network components are secured;
- Standard users and passwords on network components must be changed;
- Network segmented;
- Separation of test and production environment;
- Measures to protect end devices, servers and other infrastructure elements from unauthorised access: multi-level virus protection concept, content filter, intrusion detection system, desktop firewall, system hardening,
- Automated and regular operating system updates for server and client systems
- MDM solution on company smartphones for remote wipe/lock in the event of loss or theft
- Use of remote monitoring and management software for the centralised administration and monitoring of all client systems

### 2.3.3 Storage and use of data carriers

- Data carrier encryption with algorithms that can be classified as secure according to the current state of the art for the protection of mobile devices (notebooks, tablet PCs, smartphones, etc.) and data carriers (external hard drives, USB sticks, memory cards, etc.) is implemented using appropriate encryption software;
- Regulations for the internal and external storage of data carriers, including determination of the persons authorised to remove data carriers (key management, acknowledgement, return);
- Non-reversible deletion of data storage media and data protection-compliant disposal of data storage media that are no longer required by certified disposal companies.

#### 2.3.4 Logging of access

- Logging of instances of network access;
- Logging of instances of read access to data backups;

## 2.4 Separation control

The following measures ensure that personal data collected for different purposes is processed separately:

- INTREXX GmbH uses access authorisations to ensure that only authorised users can access the data subject to their access authorisation;
- The different data sets are separated by storing them in logically separate databases or directories;
- Separation of test, development and production systems; production data is not used for tests;
- Data collected for different purposes is processed separately;
- Any existing copies or extracts from customer databases are located on separate servers in separate databases for each customer, so that authorisation can be assigned at individual or group level for each database.

## 2.5 Pseudonymisation

Personal data must be processed in such a way that the data can no longer be assigned to a specific person without additional information.

- Pseudonymisation is implemented by INTREXX GmbH at the request and instruction of the Client in individual cases;
- Where possible: replacement of personal data (in particular names) with a pseudonym, storage of the information linking the ID and name in a separate assignment file and storage on a separate, secure IT system;
- Regularly checking as to which data can be anonymised or deleted.

## 2.6 Encryption

- An encrypted communication channel (FTPS) is available for the transmission of database copies, Intrexx portals/application exports from the Client to INTREXX GmbH;
- Notebooks are encrypted and equipped with pre-boot authentication;
- Data on smartphones is encrypted
- External data carriers that leave the company premises are generally encrypted;
-
- If you attempt to access our websites without encryption, you will be automatically redirected to encrypted access ("HTTPS").

- All websites/portals are only accessible in encrypted form

## 2.7 Further measures

- Representation rules defined and designed in accordance with authorisation;
- Regular review of access and access authorisations;
- Installation of critical and/or important security updates/patches to ensure confidentiality.

# 3. Integrity

Integrity, within the meaning of Art. 32 (1) (b) GDPR documents how attempts are made to prevent data and the information contained therein from being falsified. The two key points here are transfer control and input control.

## 3.1 Transfer control

In the case of transfer control, the company lists all measures to ensure that personal data cannot be read, copied, changed or deleted by unauthorised third parties during transport. The following measures have been implemented to ensure this:

### 3.1.1 Regulation of electronic transmission

- Documented definition of the bodies (third parties) to which data may be transmitted and the persons who are authorised to transmit it (authorisation concept);
- Options for the encrypted transmission or transfer of data are available (VPN, https, etc.);
- Data transmission and recipient of data are logged.

### 3.2.1 Regulations for the transport of data carriers

- Transport of data carriers exclusively by company-owned couriers, secure transport conditions or carefully selected service providers;
- Data carriers must always be encrypted in advance.

## 3.2 Input, storage and data carrier control

Input control should record who has entered, changed or removed the data in a data processing system. Logging should ensure that it is possible to check that data has not been falsified by unauthorised persons.

- Every employee has personal access to the IT systems based on their user name and password, coupled with the authorisations required for their purposes to access this data ("Write/Edit", "Read only", "No authorisation");

- Log data when personal data is changed, where possible;
- Traceability of changes, deletions and entries;
- No use of group accounts (including administrators or root) or one account by several employees.
- If, in exceptional cases, centralised, unprivileged accounts are used in isolated cases, they are checked via audit logs and login IPs.

# 4 Availability / resilience / recoverability

The following measures have been taken to ensure that personal data is not simply "lost" or accidentally destroyed in accordance with Art. 32 (1) (b) GDPR.

## 4.1 Data centre

### 4.1.1 Power supply

- Separate power circuit for data centre;
- The components are protected by means of an uninterruptible power supply ("UPS"), overvoltage protection and an emergency power generator.

### 4.1.2 Fire protection

- Data centres are equipped with an early fire detection system and a fire alarm system, including a direct reporting chain to the local fire brigade.
- Extinguishing system is set up according to the state of the art

### 4.1.3 Air conditioning

- Temperature monitoring
- State-of-the-art air conditioning is installed

### 4.1.4 Internet

- Internet connection with corresponding availability SLAs.

### 4.1.5 Hardware and software components

- Redundantly designed server components;
- Redundant virtual environment;
- The server and storage systems are equipped with at least a RAID-1, so that the data stored on them is available on at least two hard drives;
- Prompt replacement of defective server components as part of corresponding service contracts;

### 4.1.6 Cumulative measures

- UPS, fire and smoke detection system, manual extinguishers and air conditioning technology are subject to maintenance and service contracts.
- Monitoring of hardware, software and infrastructure components.
- Monitoring of central components and nodes of the data centre
- Water ingress protection in place
- Exclusive use of well-known manufacturers that are established on the market

## 4.2 Backup and recovery of information

- Documented data backup concept including organisational regulations for data carrier storage (labelling, retention periods);
- Automated, controlled, logged and regular complete backup of files, databases and systems in accordance with the data backup concept;
- Password protection for data backup media;
- Data backups, including the backup systems, are protected against unauthorised physical, system and data access;
- Data backup media are stored separately from the backup systems in a secure, specially protected (external) location;
- Recovery concept for the rapid recovery of files, databases and systems; regular tests for the recovery of files, databases and systems;
- Disaster recovery concept with regulations such as responsibilities, restart concepts, on-call duty, emergency organisation etc. in the event of a disaster;
- Emergency drills are carried out and documented.

## 4.3 Organisational measures

- The hardware and software used is regularly checked and, if necessary, adapted to the state of the art;

# 5. Procedures for regular review, assessment and evaluation

## 5.1 Data protection management system

The following measures are intended to ensure that an organisational system is in place that meets the basic requirements of data protection law. All elements required to ensure data protection are subject to the systematic coordination of the data protection management system.

- INTREXX GmbH has installed a data protection organisation system;
- An external data protection officer (DPO) has been appointed in writing and forms part of the data protection team. Proof of expertise and regular further training are available. Due to his/her legal obligation of confidentiality towards customers, employees, etc., he/she

must always be directly available, including to supervisory authorities. You can contact our DPO at the following email address, which only he/she can access and view: ;Datenschutzbeauftragter@intrexx.com

- A data protection directive has been issued by the controller and is supported by various guidelines from the areas of data protection and information security;
- The employees of INTREXX GmbH are regularly trained by the DPO and undergo awareness-raising measures in the areas of data protection and information security;
    - Employees are obliged to maintain confidentiality when handling personal data when they join the company;
- A register of processing activities is available and is continuously updated and audited by the DPO;
- The technical and organisational measures (TOM) have been drawn up and serve as the basis for this document, among other contributing elements;
- The effectiveness of the TOMs is regularly reviewed, assessed and evaluated to ensure the security of the processing operations;
- Subcontractors are carefully selected and are subject to regular review;
- Data subjects are provided with sufficient information regarding the processing of their personal data. Information is provided when the personal data is received or as soon as possible thereafter;
    - As part of the information provided to data subjects, reference is made to the possibility of intervention within the scope of the rights of data subjects.

## 5.2 Incident response management

The following steps have been implemented to ensure that appropriate measures are taken in the event of a data protection incident:

- Definition of reporting processes for:
    - Data protection violations pursuant to Art. 4 (12) GDPR vis-à-vis the supervisory authorities (Art. 33 GDPR);
    - Data protection violations pursuant to Art. 4 (12) GDPR vis-à-vis the data subjects (Art. 34 GDPR).
- Raising of awareness among employees regarding data protection violations;
- Documentation of data protection incidents;
- Continuous further development of reporting processes based on acquired experience.

## 5.3 Data protection-friendly default settings

Default settings must be used to ensure that personal data is only processed in accordance with the respective specific processing purpose. This applies to the quantity of personal data collected, the scope of processing, the storage period and accessibility.

- New hardware and software products are checked for data protection-friendly default settings.

### 5.4 Order control

It must be ensured that personal data that is processed on behalf of the client is only processed in accordance with the client's instructions. No order processing within the meaning of Art. 28 GDPR takes place without corresponding instructions from the client.

- Internal process and raising of awareness among employees ensures that necessary contracts for commissioned data processing are concluded;
- Agreements on commissioned data processing are concluded in writing or digitally between the Client and the Contractor. Part of the agreements is that instructions are issued in writing by the Client to the Contractor;
- Initial inspection within the meaning of Art. 28 (1) GDPR;
- In the event of changes to existing procedures or the introduction of new procedures for the processing of personal data, the data protection officer will be involved;
- Notification in the event of unlawful acquisition of personal data;
- Ongoing monitoring of the Contractor and its activities;
- Effective control rights vis-à-vis the Contractor;
- Obligation of confidentiality in the handling of personal data on the part of the Contractor's employees (Art. 5, 28, 29, 32 GDPR);
- Ensuring that the persons entrusted with data processing are familiar with the relevant data protection and client-specific regulations
- Ensuring the immediate correction, blocking and deletion of order data on the instructions of the client or after completion of the order;

## 6. Technical and organisational measures for SaaS and cloud-based products

The INTREXX SaaS/PaaS, IX 25 and IX12 products are provided via a cloud-based infrastructure housed in data centres operated by third-party providers (see Annex 2). All third-party providers are certified according to the ISO 27001 standard. For the server infrastructure, we also refer to the TOMs of our hosting partners, which include appropriate measures to protect the data centres and server rooms. These can be accessed via the following links

- badenIT: https://www.badenit.de/wp-content/uploads/2024/07/TOMs-der-badenIT.pdf

- AWS: https://aws.amazon.com/de/compliance/gdpr-center/

- Continum AG: https://www.continum.net/eu-dsgvo-bei-continum-umgesetzt/