1. Preamble

Ergon as Service Provider processes personal data within the meaning of the Federal Act on Data Protection (FADP) and the EU General Data Protection Regulation (GDPR), if GDPR is agreed or applicable as a legal basis, as well as end customer data within the meaning of the Federal Act on Banks and Saving Banks (BankG).

As part of the provision of services the Customer commissions Ergon by means of a Service, License, Project and/or Maintenance/Support contract (Main Contract) to process its personal and/or end Customer data in whole or in part. In this agreement the parties define the rules and framework conditions under which Ergon performs the data processing within the scope of the agreed service.

The following annexes form part of this agreement, whereby Annex 1 and/or 2 shall apply depending on the Services ordered in the Main Contract.

- Annex 1: Description of Data Processing – Airlock SaaS-Service
- Annex 2: Description of Data Processing – Airlock 2FA-Service
- Annex 3: Technical and Organizational Measures (TOM)

2. Subject Matter and Duration

2.1 This Data Processing Agreement supplements the Main Contract between the parties and concerns all data, details and information relating to an identified or identifiable natural person (personal data or data), including all personal data relating to the Customer's customer (end customer data).

2.2 The type of data processing within the scope of these services, the approved subprocessors and technical and organizational measures ("TOM") are set out in Annexes 1 to 3 of this agreement.

2.3 The duration of the processing shall be based on the Main Contract, unless the provisions of this agreement contains additional obligations.

3. Purpose and scope of data Processing

3.1 The type and purpose of data processing, the type of personal data and the categories of data subjects are governed by the Main Contract and the annexes to this agreement.

3.2 The Customer is owner of the data and remains entitled to all data that Ergon processes. The Customer alone determines the content, purposes and means of the processing of his personal data.

3.3 Ergon prohibits employees involved in the processing of Customer's personal data and other persons working for Ergon from processing the personal data outside of the instructions.

4. Data protection and data security

4.1 Data protection and banking secrecy

4.1.1 Ergon processes personal and end customer data exclusively in accordance with the currently valid and applicable data protection regulations.

4.1.2 If the Customer is a bank, Ergon acknowledges that the end customer data is subject to Art. 47 BankG with the corresponding penalties in the event of infringement.

4.1.3 Ergon undertakes to treat personal and end customer data as strictly confidential. The confidentiality obligations continue after the termination of the contractual relationship.

4.1.4 The employees and auxiliary personnel of Ergon involved are considered agents within the meaning of Art. 47 BankG and are obliged to comply with the confidentiality obligations (including banking secrecy). Ergon shall inform its employees, auxiliary persons and any subprocessors (together vicarious agents) of these confidentiality obligations or contractually impose these confidentiality obligations on them, insofar as they are not already subject to a statutory confidentiality obligation. Ergon shall ensure that all vicarious agents comply with data protection regulations and banking secrecy.

4.1.5 Ergon shall ensure that only those vicarious agents have access to the personal and end customer data that require it for the performance of the respective service. When selecting, instructing and monitoring the vicarious agents who have access to personal and end customer data, Ergon ensures that they comply with the law and generally perform their activities with the necessary care.

4.2 Data processing and access location

4.2.1 The processing of end customer data takes place exclusively in the region or country defined by the Customer when using the service. Neither Ergon nor its subprocessors may access end customer data outside of Switzerland. Ergon shall take appropriate technical and organizational measures to ensure this. Data processing that deviates from this provision may only take place within the scope of the existing subprocessors in accordance with Annex 1 Section (2) and/or Annex 2 Section (2) or with the prior written consent of the Customer.

4.2.2 Personal and end customer data may not be processed by Ergon in any country whose legislation does not ensure an adequate level of data protection. Data processing that deviates from this provision may only take place within the scope of existing subprocessors in accordance with Annex 1 Section (2) and/or Annex 2 Section (2) or with the prior written consent of the Customer.

4.3 Disclosure of data to third parties

4.3.1 Disclosure of personal and end customer data to third parties (not vicarious agents) is prohibited unless the Customer has given prior written consent.

4.3.2 If Ergon is required by law to process or disclose personal and end customer data to third parties, Ergon shall inform the Customer immediately unless Ergon is prohibited from doing so by law or by order of the acting authority.

4.3.3 A cross-border disclosure or transmission of personal and end customer data is prohibited unless the Customer has given prior written consent to such disclosure.

4.4 Data security

4.4.1 Ergon shall take all necessary technical and organizational measures (TOM) to ensure a level of security which is appropriate to the risks that are presented by the processing of Personal Data in accordance with Annex 3. The TOM ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. Ergon is obliged to adapt its TOM in accordance with technical advancements and development and to apply the standard of care in data processing that corresponds to the provisions on data protection and, if the Customer is a bank, on banking secrecy.

4.4.2 In the event of a data breach regarding personal or end customers data or in the event of a justified suspicion of a data breach at Ergon or a subprocessor, the reporting obligation pursuant to section 5.1.5 shall apply.

4.5 Subprocessors

4.5.1 Subprocessors are only engaged to provide the specific services agreed in the Main Contract.

4.5.2 The existing subprocessors are listed in Annex 1, section (2) and Annex 2, section (2). The Customer accepts these subprocessors.

4.5.3 Ergon shall notify the Customer prior to the engagement or replacement of a subprocessor and within 14 days the Customer may object for good cause. If no objection is raised within this period, consent to the engagement or replacement of a subprocessor shall be deemed to have been given. In the event of an objection, the Customer shall be granted an extraordinary right of termination unless an amicable solution can be found between the parties.

4.5.4 All agreements on data processing between Ergon and the Customer also apply to a subprocessor (in accordance with section 4.1.4). In any case, the subprocessor must be able to provide at least the same level of data protection as Ergon.

4.5.5 Upon request, the Customer shall be granted access to the relevant passages of the contracts between Ergon and the subcontractor regarding data protection obligations.

4.5.6 The responsibilities of Ergon and the subprocessors are clearly delineated.

4.5.7 If the subprocessor fails to comply with its data protection obligations, Ergon shall be liable to the Customer for compliance with the obligations of the subprocessor in accordance with section 7.2.

5. Support and notification obligations of the Service Provider

5.1 Ergon shall forward any requests for rectification, erasure, access or other rights by data subjects to the Customer without delay. Such requests shall be answered exclusively by the Customer. Ergon shall not be liable if requests from the data subject are not answered, not answered correctly or not answered on time by the Customer.

5.2 Ergon undertakes to support the Customer in meeting its obligations arising from statutory and regulatory provisions on data protection and banking secrecy in return for reasonable compensation (e.g. in responding to requests from data subjects or in preparing data protection impact assessments.) For this purpose Ergon shall provide the Customer with all necessary and available information.

5.3 If the Customer is subject to an inspection by supervisory authorities or other bodies or if data subjects exercise their rights, Ergon undertakes to support the Customer to the extent necessary in return for reasonable compensation. If material breaches of this agreement or deficiencies in the implementation of Ergon's obligations are identified after submission of evidence or reports following inspections, Ergon shall implement appropriate corrective measures immediately and free of charge.

5.4 If Ergon is unable to fulfill its obligations under this agreement, Ergon shall inform the Customer immediately and agree on how to proceed.

5.5 In the event of a (potential) data breach, Ergon shall notify the Customer immediately (in accordance with Art. 24 para. 3 FADP resp. Art. 33 para. 2 GDPR). Ergon shall inform the Customer in writing about the nature and extent of the breach and about the measures taken and/or to be taken to secure the data and mitigate possible negative consequences. Ergon shall immediately communicate with the Customer.

6. Rights and obligations of the Customer

6.1 Right to issue instructions

6.1.1 Any instructions issued by the Customer regarding data processing shall be documented in the main contract. The Customer is entitled to issue further instructions in writing at any time in return for reasonable compensation.

6.1.2 Ergon is entitled to suspend the implementation of an instruction which it considers to be in breach of applicable law until the legality is confirmed or the instruction is changed by the Customer. Ergon shall inform the Customer of this immediately.

6.2 Rights of access and control

6.2.1 The Customer is entitled to check the compliance with this agreement at Ergon's premises, in particular by obtaining information and reviewing the confidentiality declarations of the employees, the stored data, the Customer-specific data processing programs and other mutually agreed inspections.

6.2.2 Ergon shall allow the persons entrusted with the inspection access and insight as far as necessary and shall cooperate appropriately. The Customer and Ergon shall agree in advance on the time, duration and subject matter of the inspections and on applicable security and confidentiality provisions. The inspections shall be carried out in such a way that Ergon's operations are not unduly disrupted. The Customer's inspections are generally limited to two working days per year.

6.2.3 Each party shall bear the costs arising from inspections itself.

7. Diligence (Care), liability and damages

7.1 The parties undertake to carry out their activities to the best of their knowledge and belief by appropriately trained specialist personnel in compliance with the industry standard.

7.2 Ergon shall be liable to the Customer for any culpable breach of this agreement. The scope of liability under this agreement shall be governed exclusively by the liability provisions and limitations under the Main Contract. Further mandatory statutory liability claims remain reserved.

8. Obligations after the termination of the contract

8.1 Upon termination of the respective contractual relationship, Ergon is obliged to immediately hand over to the Customer or irrevocably delete or destroy all personal and end customer data received in connection with the provision of its services. This does not apply to backups on long-term data carriers, which are destroyed in the usual cycle. Other documents, materials and similar items must be returned or destroyed at the Customer's request.

8.2 The deletion or destruction and any return of the storage media, documents and materials must be confirmed in writing (e-mail is sufficient) by Ergon at the Customer's request.

9. Final provisions

9.1 Amendments and modifications to this agreement and all its components require a written agreement, which may also be made in an electronic format (text form), and an express reference to the fact that this is an amendment or modification to these terms and conditions. This also applies to the waiver of this formal requirement.

9.2 This Agreement shall be governed by Swiss law, to the exclusion of the UN Convention on Contracts for the International Sale of Goods dated April 11, 1980. The place of jurisdiction is determined by the information in the main contract and if no provision has been made, the exclusive place of jurisdiction is Zurich (Zurich 1), Switzerland.

10. Signatures

The contracting parties hereby agree to this agreement on data processing.

Ergon Informatik AG

Place, Date: _____ Signature: _____

Place, Date: _____ Signature: _____

Customer:

Place, Date: _____ Signature: _____

Place, Date: _____ Signature: _____

Annex 1: Description of Data Processing – Airlock SaaS-Services

(1) Type of processed personal data and categories of data subjects

The Customer acknowledges that the use of Airlock SaaS-Services requires Administration Users to provide Ergon with certain information, which may include personal information about the administration users (such as IP addresses, usernames, first and last names, passwords, email addresses and/or telephone numbers), solely for the purpose of providing and improving the Airlock SaaS-Services.

User data is processed when using the Airlock SaaS-Service. It is the responsibility of the Customer to determine which personal data (e.g. first and last names, passwords, e-mail addresses and/or telephone numbers) are processed in the configuration of the Airlock SaaS-Service, and Ergon is deemed to have been commissioned to process this data. Furthermore, the following user data is collected in any case and used for the provision of the Airlock SaaS-Services: IP addresses, user names, passwords.

Before the Customer authorizes a person as a user (administration user or user of the Airlock SaaS-Service), the Customer is fully responsible for obtaining the consent of this person in accordance with the applicable law for the use of their user data by Ergon. The Customer represents and warrants that all such consents have been or will be obtained before authorizing any person as a user.

Ergon may process, use and share certain service attributes (e.g. user activities, log files, other data associated with the Airlock SaaS-Services) for internal business purposes, e.g. to support the proper functioning of the Airlock SaaS-Services, to provide support services to the Customer and to investigate fraud, abuse or violations of the terms of use. Ergon may also process, share, reproduce or otherwise use Airlock SaaS-Services attributes and Customer data in the form of anonymized data for internal business purposes (such as improvements to the Airlock SaaS-Services) or as aggregated data for marketing purposes (with the exception of the direct sale of Customer data to third parties) and subject to the Customer's confidentiality requirements agreed. Anonymized data means attributes of the Airlock SaaS-Services and/or Customer data from which the following information has been removed: personally identifiable information and the names and addresses of the Customer and its Users.

(2) Subprocessors

To support the provision of the Airlock SaaS-Services, Ergon may engage and utilize data processors with access to some Customer data (each a “subprocessor”). The table below contains information about the identity, location and role of each subprocessor. Where multiple data processing locations are listed, data processing will take place at the location specified in the Main Contract, otherwise at all the locations listed below.

Company, Unit	Purpose of data processing	Place of data processing	Description
Microsoft, Azure	Primary supplier for the cloud infrastructure for the Airlock SaaS-Services	EU, Switzerland	Various Azure services, including storage, processing and backup of Airlock SaaS Services data.
MongoDB, MongoDB Atlas	Database for administration of	Switzerland	Storage of data in connection with the provision, administration and configuration of Airlock SaaS-

	Airlock SaaS-Services		Services, including data of administration users.
HashiCorp, HCP Vault	Digital key management	Switzerland	Secure management of keys and security-relevant data, for infrastructure components as well as for services for the Customer.
Twilio, SMS	Sending of SMS	USA	SMS gateway for sending OTP for administration users and users of non-production services for the Customer.
Twilio, Sendgrid	Sending of emails	USA	Email gateway for sending OTP and notifications for administration users and users of non-production services for the Customer.
Futurae Technologies AG	Provider of the Airlock 2FA service	EU, Switzerland	Processing of device data, internet traffic data, message payload and other data related to the 2FA service as detailed in Annex 2, Section (1).
PagerDuty Inc, PagerDuty	Incident management	USA	Preparation of service status information and management of incidents.
ZoHo Corp. – ManageEngine 5200 Franklin Dr, Suite 115 Pleasanton, CA 94588 USA	Infrastructure Monitoring	Globally Mirrored Data Centers: North America: Seattle and Dallas Europe: Amsterdam and Dublin India: Chennai and Mumbai China: Shanghai Australia: Sydney and Melbourne	Site24x7 – Infrastructure Monitoring

As the Airlock SaaS-Services evolve, the subprocessors we engage may also change and will be updated in accordance with (4.5.3) in this agreement. Before we engage a new subprocessor, we will carefully review its privacy, security and confidentiality practices and enter into an agreement to implement these obligations.

Annex 2: Description of Data Processing – Airlock 2FA-Service

(1) Type of processed personal data and categories of data subject

Question	Answer
Categories of data subjects whose Personal Data is being processed	Natural persons which (i) access or use the Airlock 2FA-Service or (ii) are Customer's personnel, partners, vendors or agents, in each case accessing or using the Airlock 2FA-Service (End Users).
Categories of Personal Data processed	Profile or contact data: Ergon processes this information (for example, Name, Email, Phone number, Account password) directly from End Users, when they choose to give it to us expressly (such as when signing up for an account) or when Customer determines in its sole discretion to make it available to Ergon as part of the Airlock 2FA-Service (for example, Username, Randomly Generated Identifier, Cryptographic Key) to enable Ergon to provide the Airlock 2FA-Service and perform the Main Contract. Device Data: Ergon processes this information (for example, Type of device used to access the Airlock 2FA-Service, Operating system), pseudonymized from End Users when they choose to give it to Ergon expressly as part of the Airlock 2FA-Service or automatically when End Users choose to use certain Airlock 2FA-Service such as Futurae Adaptive (for example, Geolocation, WiFi networks scan, Bluetooth devices scan, Connected WiFi network, Connected Bluetooth devices, Connected devices in the same network, Device sensors, Nearby devices), in each case to enable Ergon to provide the Airlock 2FA-Service and perform the Main Contract. Internet Traffic Data: Ergon processes this information (for example, network traffic data such as IP address, browser and browser fingerprint, domain, time stamp, cookie or referring web address) automatically when End Users choose to give it to Ergon expressly as part of the Airlock 2FA-Service,

	to enable Ergon to provide the Airlock 2FA-Service and perform the Main Contract. Usage Data: Ergon processes this information (for example, how often various service features are used, inferences drawn from service usage data) automatically when End Users use the Airlock 2FA-Service, to understand feature usage and improve our Airlock 2FA-Service.
Sensitive data transferred (if applicable) Restrictions or safeguards that take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions, keeping a record of access to the data, restrictions for onward transfers or additional security measures	No sensitive data. Data shall be protected by applying the security measures described in Annex 3.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)	Continuous for the duration of the Main Agreement.
Nature of the processing	Processing necessary to provide the Airlock 2FA-Service to Customer and End Users in accordance with the Main Agreement, this DPA and the documented instructions provided.
Purpose(s) of the data transfer and further processing	Processing necessary to provide the Airlock 2FA-Service to Customer and End User in accordance with the Main Agreement, this DPA and documented instructions provided.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period	Until (i) expiry/termination of the Main Agreement, or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Main Agreement (to the extent applicable, whichever is latest).
For transfers to subprocessors, also specify subject matter and nature of the processing	The subject matter and nature and duration of the processing shall be as specified section (2) below.

(2) Subprocessors

To support the provision of the Airlock 2FA-Service, Ergon may engage and utilize data processors with access to some Customer data (each a "subprocessor"). The table below contains information about the identity, location and role of each subprocessor. Where multiple data processing locations are listed, data processing will take place at the location specified in the Main Contract, otherwise at all the locations listed below.

Company	**Purpose of data processing**	**Place of data processing**	**Description**
Futurae Technologies AG	Provider of the Airlock 2FA service	EU, Switzerland	Processing of device data, internet traffic data, message payload and other data related to the 2FA service as detailed in Annex 2, Section (1).
Google Cloud EMEA Limited	Primary cloud infrastructure provider of Futurae	EU, Switzerland	Various activities including storage, computation and backup of Airlock 2FA-Service data.
Cloudflare, Inc.	Web Application Firewall (WAF), Anti-DDoS (Distributed Denial of Service) for Futurae	Global	Various activities pertaining to the security, performance, and reliability of the Airlock 2FA-Service. This subprocessor is required to ensure high reliability and availability of the Airlock 2FA-Service, including resistance against advanced network attacks, such as Distributed Denial-of-Service (DDoS). The encrypted TLS connection is terminated to

			detect attacks at the application level.
Akenes SA (Switzerland)	Futurae services: Third-party hosting provider	Switzerland	Hosting provider for legacy Services only - in course of being completely decommissioned

As the Airlock 2FA-Service evolves, the subprocessors we engage may also change and will be updated in accordance with (4.5.3) in this agreement. Before we engage a new subprocessor, we will carefully review its privacy, security and confidentiality practices and enter into an agreement to implement these obligations.

Annex 3: Technical and Organizational Meaures (TOM)

This Annex describes the technical and organizational measures taken by Ergon regarding the Airlock SaaS Service in accordance with applicable data protection law to implement an adequate level of protection for the personal data processed by Ergon under the Main Contract.

Airlock SaaS has implemented and will maintain an information security program. The program aims to be certified under the ISO/IEC 27001 standard. This security program includes the following measures and processes:

1. Confidentiality

1.1 Measures for access control of data processing centers

i. Operational task restrictions: Policies are implemented to restrict operational tasks to be performed exclusively within Switzerland, ensuring data protection and compliance.

ii. Physical security of office workplaces: Implementation of protective measures such as window privacy filters and physical access controls.

iii. Remote work security policies: Policies to delegate enforcement of similar security measures for home offices, ensuring compliance with organizational data protection standards.

1.2 Measures for access control of data processing systems

i. Restricted access: Access to systems processing personal data is restricted to individual user accounts with mandatory multi-factor authentication.

ii. Privileged access management solution: Access to systems processing personal data is protected through a privileged access management (PAM) solution.

iii. Strict access control rules for critical components: The four-eyes principle is employed for all operations tasks on production environments which could be used to perform changes or read / modify PII data.

1.3 Measures for access control of personal data in data processing systems

i. Access request reviews: A formal review procedure is in place for any access requests involving critical privileges, ensuring that such requests are thoroughly assessed and approved.

ii. Encryption at rest: Full disk encryption on all systems storing personal or customer data.

iii. Protection of low-entropy user secrets: Low-entropy secrets (e.g. passwords) are protected by cryptographic techniques, such as salting and resource-intensive key derivation functions.

iv. Code review enforcement: All changes undergo mandatory code reviews to ensure adequate quality and security before deployment.

v. Access control reviews: Regular reviews are conducted for any modifications to the access control configuration of the cloud infrastructure, ensuring that access remains secure and aligned with the principle of least privilege.

1.4 Measures of separation control

i. Database access controls: Tenant level database separation and access controls following least privilege principles.

ii. Service access protection: Network-level micro segmentation with authentication based on certificates and workload identities.

iii. Web-specific security measures: Cross-tenant access or manipulations are mitigated using appropriate web specific protections.

iv. Test Environments: Full separation of test and production environments.

v. Controlled build infrastructure: Controlled and trusted build infrastructure with temporary build environments.

2. Integrity

2.1 Measures of transfer control

i. Encryption in transit: Secure network communication using TLS, or protocols with equivalent security guarantees for any network connection spanning multiple compute nodes that may contain personal data, except in cases where:

- data and/or metadata are transmitted via email or SMS, which may rely on plain-text channels beyond the control of Airlock SaaS Service; to mitigate the associated risk, a security review is required and additional protections (e.g. short-lived tokens) are implemented when the transmission involves personal data or secrets.

ii. Public key cryptography: Use of public key cryptography to generate and verify signatures to guarantee the integrity of temporary data stored by clients (e.g. access tokens).

iii. Authenticated encryption: Authenticated encryption algorithms are employed to protect the confidentiality and integrity of data stored on the client, ensuring data remains secure and unmodified.

iv. Declarative infrastructure definitions: Infrastructure as code is used for all changes to the cloud infrastructure, ensuring that changes are consistent, repeatable, and version-controlled.

2.2 Input control measures

i. Log retention: Non-debug logs for Airlock SaaS tenants are retained for at least 365 days in production environments and at least 30 days in non-production environments.

ii. Immutable logs: Audit logs are stored in immutable log systems with the same retention on Airlock SaaS tenants, and between 30 days and 13 months for any actions performed by SaaS administrators depending on the capabilities of the related system.

iii. Automated deployments: Deployments, including IAM configurations and secrets, are fully automated to support reproducible deployments, reducing human error and maintaining consistency.

3. Procedures for regular review, assessment and evaluation

3.1 Data Protection Management

i. Regular training: Regular training for all employees with access to PII with regards to data protection policies and laws.

ii. Data protection roles: Positions for Information Security Officer and Data Protection Officer are defined and communicated.

iii. Records of processing activities: Maintaining a record of processing activities in accordance with GDPR Art. 30.

3.2 Incident Response Management

i. Incident response process: Documented and trained incident response process with escalations for security incidents and crisis management.

ii. Data protection violation process: Established process to communicate violations of data protection laws with the appropriate authorities.

3.3 Order control

i. Background checks: Industry-standard background checks are conducted for all employees with privileged access to personal data to verify trustworthiness.

ii. Trained SaaS partners: Only professionally trained SaaS partners with access to specialized documentation are allowed to deploy on the Airlock SaaS platform, ensuring they meet specific deployment requirements.

iii. Clear role definitions: The roles and responsibilities of the Airlock SaaS platform team, the SaaS partner, and the customer are clearly defined to prevent ambiguity and assign accountability.

iv. Security awareness training: Ergon provides general security awareness training for all employees and specific trainings for any person with operations responsibilities related to personal data.

v. Specialist support: Contracted external specialists for communication with authorities and threat actors.

vi. Auditability: Airlock maintains documentation on changes and incidents regarding the security of the SaaS platform to allow auditing.

vii. Delegation of duties: Airlock takes reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set out in this document.

4. Availability and resilience

4.1 Availability control

viii. Monitoring and alerting: Appropriate monitoring mechanisms are deployed to continuously track Service performance compliant with agreed SLAs. Deviations trigger alerts to operations personnel for immediate attention and resolution.

ix. Disaster recovery and business continuity plans: Adequate plans and procedures are implemented, addressing target recovery time and recovery point objectives to enable minimal disruption.

x. Encrypted backup storage: Encrypted backups are stored across multiple sites to safeguard against data loss and ensure availability.

xi. Regular testing: Periodic recovery and resilience tests are conducted to verify the effectiveness of disaster recovery measures and ensure systems can withstand disruptions.