Data Processing Agreement der Cronon GmbH

1. Scope and applicable Data Protection Laws

(1.1.) This data processing agreement (»Agreement«) is concluded between the Customer (hereinafter referred to as the »Customer«) and the relevant company of the IONOS Group SE and their affiliates (hereinafter referred to as the »Processor«), with which the Customer has accepted the General Terms and Conditions (hereinafter referred to as the »GTC«), together referred to as the »Parties«. The identity of the Processor can be found in the aforementioned GTC.

In this Agreement, the following definitions apply:

(1.1.1.) Data Protection Laws means:

(1.1.1.1.) In instances where the General Data Protection Regulation of the European Union is applicable, the legal framework for data protection within the European Union or the specific member state to which either the Customer or the Processor is subject shall govern.
(1.1.1.2.) In instances where the UK GDPR is applicable, the legal framework for data protection within the United Kingdom shall govern.

(1.1.2). EU GDPR means the General Data Protection Regulations ((EU) 2016/679) hereinafter referred to as the »GDPR«.

(1.1.3.) UK GDPR has the meaning given to it in section 3 (10) (as supplemented by section 205(4)) of the Data Protection Act 2018, hereinafter referred to as the »UK GDPR«.

(1.2.) Pursuant to this Agreement, the Parties hereby agree that the terms »controller,« »data subject,« »personal data,« »processing,« »processor,« and »third party/ies« shall be defined in accordance with the prevailing Data Protection law.

2. Subject-Matter And Duration Of The Processing

(2.1.) This Agreement sets out the respective data protection rights and obligations of the parties in relation to the provision of services in accordance with the Description of Service, Terms of Services and GTC (hereinafter referred to as the »Main Contract«). This Agreement applies to the extent that the Processor processes personal data on behalf of the Customer as controller. This includes all activities that the Processor performs to fulfil the Main Contract and that represent a data processing activity on behalf of the Customer. This Agreement shall apply to any instructions from the Customer, regardless of whether such order or instruction explicitly refers to this Agreement.

(2.2.) The duration of the processing corresponds to the actual processing of the Customer's personal data by the Processor.

3. Nature and purpose of the processing

(3.1.) The nature of the processing includes all types of processing as defined by the Data Protection Law to fulfill the Main Contract.

(3.2.) Purposes of processing are all purposes required to provide the contracted services (see also Description of Service in Appendix 1) in particular in terms of cloud services, hosting and IT support.

4. Type of personal data and categories of data subjects

(4.1.) The type of processed data is determined by the Customer by the product selection, the configuration, the use of the services, and the transmission of data. See also the Description of Service in Appendix 1.

(4.2.) The categories of data subjects are determined by the Customer via product selection, configuration, the use of the services, and the transmission of data. See also the Description of Service in Appendix 1.

5. Responsibility and processing on documented instructions

(5.1.) The Customer is solely responsible for complying with the legal requirements of the applicable Data Protection Laws, in particular, the legality of the transfer of data to the Processor and the legality of data processing under this Agreement. This also applies to the purposes and means of processing set out in this Agreement.

(5.2.) The instructions are initially determined by the Main Contract and can then be changed by the Customer in writing or in an electronic format (text form) by individual instructions (individual instruction). Verbal instructions must be confirmed immediately in writing or in text form. In the event of proposed changes, the Processor shall inform the Customer of the effects that this will have on the agreed services, in particular, the possibility of providing services, deadlines, and remuneration. If the implementation of the instruction is not reasonable to the Processor, the Processor is entitled to terminate the processing and give extraordinary notice of termination of the contract. The Customer's obligation to pay shall cease upon the Processor's termination of the service. Unacceptability exists in particular if the services are provided in an infrastructure that is used by several Customers of the Processor (shared services), and a change in the processing for an individual Customers is not possible or is unreasonable.

(5.3.) The contractually agreed data processing location is determined by the Processor's establishment as follows:

(5.3.1.) if the Processor is established within a Member State of the European Union or in the European Economic Area, in a Member State of the European Union or in another contracting state to the Agreement on the European Economic Area, or

(5.3.2.) if the Processor is established within the United Kingdom, in the United Kingdom,

(5.3.3.) Notwithstanding the above, unless the transfer of data to third countries becomes necessary in order to provide the service. In the event that a transfer to a third country takes place, the Processor shall ensure that the relevant Data Protection Laws requirements are fulfilled.

6. Rights of the Customer, obligations of the Processor

(6.1.) The Processor may only process data of data subjects only within the framework of the order and on the basis of documented instructions of the Customer. The Main Contract specifies and determines the instructions.

(6.2.) Notwithstanding any other provision of this Agreement, if the Processor is under a mandatory legal obligation pursuant to the local applicable law of the European Union, the law of an European Union Member State, or the law of the United Kingdom to process Personal Data in a manner that deviates from the documented instructions of the Customer, the Processor shall comply with such legal obligation. In such an event, the mandatory legal requirement shall supersede the Customer's instructions. The Processor shall, to the extent permitted by law, inform the Customer of such legal obligation prior to processing the personal data in deviation from the Customer's instructions. Unless the law in question prohibits such information.

(6.3.) The Processor shall inform the Customer without delay if it considers that an instruction violates applicable laws. The Processor may suspend the implementation of the instruction until it has been confirmed or modified by the Customer. The instructions shall be documented by the Customer and kept for at least the duration of the contractual relationship.

(6.4.) In the light of the nature of the processing, the Processor shall, as far as possible, assist the Customer with appropriate technical and organisational measures in order to fulfil the rights of the data subjects laid down in the applicable Data Protection Laws. The Processor is entitled to demand appropriate compensation from the Customer for these services. The Processor shall provide the Customer with cost information in advance, except when the support is required due to a breach of law or contract by the Processor.

(6.5.) The Processor shall assist the Customer in ensuring compliance with the obligations pursuant to the applicable Data Protection Laws as controller, especially regarding the security of processing, data breaches, data protection impact assessments, prior consultation with supervisory authorities, taking into account the nature of processing and the information available to the Processor. The Processor is entitled to demand appropriate compensation from the Customer for these services, insofar as the support was not required due to a breach of law or contract by the Processor. The Processor shall provide the Customer with cost information in advance.

(6.6.) The Processor ensures that the employees involved in the processing of the data of the Customer and other persons acting on behalf of the Processor are prohibited from processing the data outside the instruction issued. Furthermore, the Processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The obligation of confidentiality remains even after the order has been completed.

(6.7.) The Processor ensures that persons authorized to process personal data have committed themselves to confidentiality or are under an appropriate statutory, professional, or other applicable legal obligation of confidentiality, including specific national secrecy laws in regard of, but not limited to telecommunication and professional secrecy. The obligation of secrecy remains even after the order has been completed.

(6.8.) The Processor shall inform the Customer immediately if the Processor becomes aware of violations of the protection of personal data of the Customer. The Processor shall take the necessary measures to safeguard the data and to mitigate possible adverse consequences for the data subjects.

(6.9.) The Processor guarantees the written appointment of a Data Protection Officer, who shall carry out their activity in accordance with the applicable Data Protection Law. A contact option will be published on the website of the Processor.

(6.10.) At the end of the provision of the processing services, the Processor will, at the choice of the Customer, either delete or return the personal data, unless there is an obligation under applicable European Union or national law of a member state of the European Union or the law of the United Kingdom to retain the personal data. If the Customer does not exercise this option, deletion is deemed agreed. If the Customer chooses to return, the Processor can demand a reasonable compensation. The Processor shall provide the Customer with cost information in advance.

(6.11.) If a data subject asserts claims for compensation according to the applicable Data Protection Laws, the Processor shall support the Customer in defending the claims within the scope of its possibilities. The Processor may demand reasonable compensation for this, insofar as the claims for damages are not based on a breach of law or contract by the Processor.

7. Obligations of the Customer

(7.1.) The Customer must immediately and completely inform the Processor if the Customer identifies errors or irregularities with regard to the applicable Data Protection Law when carrying out the order.

(7.2.) In the event of termination, the Customer undertakes to delete personal data which it has stored during its service, before the termination of the contract.

(7.3.) At the request of the Processor, the Customer appoints a contact person for data protection matters.

8. Requests from the data subjects

The Processor shall promptly inform the Customer of any request received from the data subject. The Processor shall not respond to the request himself, unless the Processor has been authorized to do so by the Customer. Taking into account the nature of the processing, the Processor shall assist the Customer in fulfilling the Customer's obligation to respond to requests from data subjects to exercise their rights. In fulfilling its duties, the Processor shall follow the instructions of the Customer. The Processor shall not be liable if the request of the data subject is not answered by the Customer, not answered correctly or not answered in due time.

9. Measures for the security of processing

(9.1.) The Processor will take appropriate technical and organisational measures in its area of responsibility to ensure that the processing is carried out in accordance with the requirements of the applicable Data Protection Laws and ensure the protection of the rights and freedoms of the data subjects. The Processor shall take appropriate technical and organisational measures to ensure the confidentiality, integrity, availability and resilience of the processing systems and services in the long term.

(9.2.) The specific technical and organizational measures implemented by the Processor are set out in Appendix 2 of this Agreement.

(9.3.) The Processor shall conduct periodic assessments of the efficacy of the technical and organizational safeguards implemented to ensure the security of processing in compliance with the applicable Data Protection Law.

(9.4.) The Processor reserves the right to modify the implemented technical and organizational measures in accordance with advancements in technology and evolving risk landscapes. Such modifications are permissible provided that the level of data protection required by applicable Data Protection Laws is consistently maintained and not diminished.

10. Proof and verification

(10.1.) The Processor shall provide the Customer with all the information necessary to prove compliance with the obligations laid down in the applicable Data Protection Laws and shall allow and contribute to audits, including inspections, carried out by the Customer or another auditor appointed by the Customer. The Processor reserves the right to require a confidentiality undertaking from the Customer and its designated auditor, which shall not preclude the Customer from providing evidence to the competent supervisory authority. The Processor may reject direct competitors of the Customer or persons who work for direct competitors of the Customer as auditors.

(10.2.) As proof of compliance with the obligations of the applicable Data Protection Laws, the existing certification in accordance with ISO 27001 is generally sufficient for the Customer. The Processor shall make the current certificate available on its website.

(10.3.) In cases where the Customer has legitimate concerns, based on factual evidence, that the provided certifications regarding data protection and security measures are insufficient or inappropriate, or if data breaches occur in connection with the data processing activities carried out on behalf of the Customer, the Customer reserves the right to conduct inspections.

(10.4.) The Customer will provide reasonable notice of any such inspections and will conduct them in a manner that minimizes disruption to the Processor's operations. The Customer's inspection right is limited to verifying the Processor’s compliance with its obligations under the applicable Data Protection Laws and this Agreement. The Processor will use all reasonable efforts to facilitate and assist the Customer with such inspection.

(10.5.) The Processor may require reasonable compensation for information and assistance, insofar as the inspection was not required because of a breach of law or contract by the Processor. The Processor shall provide the Customer with cost information in advance.

11. Subprocessors (other processors)

(11.1.) The Customer grants the Processor general authorization to engage other processors (»Subprocessors«) for the fulfillment of the Main Contract. A current list of these Subprocessors will be made available to the Customer upon request. The Customer agrees to the Subprocessors currently engaged by entering into this Agreement.

(11.2.) The Processor shall inform the Customer in text form (e.g., via email) of any intended addition or replacement of Subprocessors.

(11.3.) The Customer may object to such changes within a period of 14 days from receipt of the notification. The objection must be submitted in text form and requires a justified ground related to data protection law. If the Customer does not object within this period, the change shall be deemed approved. If the Customer objects on reasonable grounds and the Parties cannot reach an amicable solution, the Processor is entitled to terminate the affected services with a notice period of 14 days, provided that the Processor cannot reasonably provide the service without the new Subprocessor. In this case, the Customer's payment obligation ends upon discontinuation of the service.

(11.4.) Where the Processor engages Subprocessors, it shall impose data protection obligations upon them that are no less protective than those set out in this Agreement. The Processor remains fully liable to the Customer for the performance of the Subprocessor's data protection obligations.

12. Liability and compensation

(12.1.) In the event that a data subject asserts a claim for compensation under the applicable Data Protection Law, both Parties agree to assist each other and contribute to clarifying the underlying facts.

(12.2.) The liability provision as agreed between the Parties in the Main Contract for the provision of services shall also apply to claims arising from this Agreement and in the internal relationship between the Parties for claims of third parties under the applicable Data Protection Laws, unless expressly agreed otherwise.

13. Contract period, miscellaneous

(13.1.) This Agreement begins when the Customer executes the Main Contract. It ends with the termination of the last contract under the respective Customer number. If any data processing on behalf of the Customer still takes place after termination of this contract, the regulations of this Agreement are valid until the actual end of the processing.

(13.2.) The Processor may amend the Agreement at its reasonable discretion with reasonable notice. In particular, the Processor expressly reserves the right to unilaterally amend this agreement if major legal changes in relation to this agreement occur. The Processor shall separately inform the Customer of the significance of the planned amendment and shall furthermore grant the Customer a reasonable period of time to declare an objection. The Processor shall inform the Customer in the notice of amendment that the amendment will become effective if the Customer does not object within the set period. In the event of an objection by the Customer, the Processor shall have an extraordinary right of termination.

(13.3.) The Customer acknowledges this Agreement as part of the GTC of the Processor, concerning the product(s) booked by the Customer. In the event of any contradictions, the provisions of this Agreement for data processing(s) shall prevail to the provisions of the Main Contract. Should individual parts of this Agreement be ineffective, this does not affect the validity of the remaining provisions of the Agreement.

(13.4.) This Agreement shall be governed by the same laws and jurisdiction as set forth in the GTC.

(13.5.) If the data of the Customer is endangered by seizure or confiscation, by a bankruptcy or settlement procedure, or by other events or measures of third parties, the Processor shall inform the Customer immediately. The Processor will inform all persons responsible in this connection without delay that the sovereignty and the ownership of the data lie exclusively with the Customer.

Appendix 1

1. Subject Matter and Duration of Processing

The subject matter of the processing is derived from the Main Contract concluded between the Parties and the associated Service Specifications (»Product Information«). The duration of the processing corresponds to the term of the Main Contract.

2. Nature and Purpose of Processing

The processing is carried out for the purpose of providing IT infrastructure, data center services, cloud platforms, and managed services in accordance with the Main Contract. Depending on the specific product or service booked, the nature of the processing includes:

- **Infrastructure & Hosting:** Storage, physical hosting, and virtualization of data and systems within the Processor's data centers.
- **Connectivity:** Transmission of data via the network, routing, and provision of internet access.
- **Managed Services & Support:** Administration, maintenance, monitoring, and technical support of operating systems, databases, and applications.
- **Security & Availability:** Processing for the purpose of system security (e.g., firewalling, DDoS protection) and data availability (e.g., creation of backups), provided these are part of the agreed services.

3. Categories of Data Subjects

The categories of data subjects are determined exclusively by the Customer based on their specific use of the services. Since the Processor provides technical infrastructure for the Customer's various business purposes, these categories typically include, but are not limited to:

- Customers, interested parties, and business partners of the Customer.
- Employees, freelancers, and agents of the Customer (e.g., system users, administrators).
- Users of the Customer's websites, applications, or networks.

4. Categories of Personal Data

The specific types of personal data are determined by the Customer's use of the services.
The data processed generally falls into the following technical categories:

- **Content Data:** Any data that the Customer stores, processes, or transmits on the Processor's systems (e.g., database contents, files, emails, website content). The Processor generally has no influence over the specific content; this may include any category of personal data, including special categories of data pursuant to Art. 9 GDPR, as defined by the Customer.

- **Usage and Traffic Data:** Technical data generated during the use of the services and the operation of the network infrastructure (e.g., IP addresses, access logs, time stamps, telemetry data, and other technical metadata required for service delivery and security).
- **Administrative and Access Data:** Data required for the administration of and access to the systems (e.g., user IDs, SSH keys, authentication certificates, and technical contact information).

Appendix 2 – Technical and Organizational Measures (Version 1 / August 2025)

1. Physical Security of the Infrastructure

1.1 Access Control and Management

- **Access is restricted to authorized individuals.**
- **Access Rights Management:** A process for issuing and withdrawing access rights is implemented, with a role-based approach to assigning access authorizations.
- **Advanced Authentication:** Advanced methods, such as two-factor authentication, are implemented.
- **Logging of Entries and Exits of Security Zones**

1.2 Security Zone Planning and Perimeter Protection:

- **Security Zone Planning:** A security zone concept and plan is developed and regularly maintained, with rooms and spaces assigned to designated zones. Each Zone requires certain security measures.
- **Physical Barriers:** Physical barriers like fences, walls, and secure gates are established to protect the facility's boundaries.

1.3 Alarm and Detection Systems

- **CCTV and Notification Systems:** CCTV systems are installed for infrastructure monitoring, paired with automatic notification systems for threat detection.
- **Alarm Systems:** Alarm systems are deployed to detect fire, water leaks, and unauthorized access, providing automated alerts to security personnel and emergency services.

1.4 Protection Against Environmental Dangers

- **Critical Supply Line Maintenance:** Maintenance encompasses both the layout plans and the physical infrastructure of critical supply lines (electricity, water, telecommunications) to prevent disruptions.
- **Air Conditioning and Redundancy Measures:** Air conditioning systems and redundancy measures for power and cooling are implemented to ensure infrastructure continuity.

1.5 Visitor and External Personnel Regulations

- **Visitor Management:** Strict visitor rules, including the use of visitor badges and accompanied access, are in place.

2. Rights and Roles-Concept

The following measures are implemented to ensure that users only have access to the personal data necessary for their specific tasks:

2.1 User ID Requirements

- **Unique User IDs:** User IDs are unique, as they are not reused or duplicated, ensuring individual accountability and traceability within the systems.
- **Prohibition of Non-Personalized Accounts**

2.2 Granting and Revoking of Authorizations

- **Dual Control Principle:** A dual control approach is implemented for critical resources, ensuring that the processes of access authorization and allocation of rights are kept separate.
- **Role-Based Access Control:** Access to resources is systematically allocated based on predefined regulations, with clearly defined roles established by the resource responsible person.
- **Need-to-Know and Need-to-Do Principle:** Access rights are granted following the principles of »need-to-know« and »need-to-do«.
- **Formal Authorization Processes:** Formal processes are established for granting and revoking authorization.
- **Timely Revocation of Access Rights:** Access rights are revoked promptly when they are no longer needed.

2.3 Authorization Review and Documentation

- **Creation and Maintenance of Authorization Repositories:** Repositories are created and maintained to document assigned responsibilities and authorization concepts for information, systems, and applications.
- **Traceable Documentation of User Account Actions:** Actions related to the creation, modification, and deactivation of user accounts, along with any adjustments to access rights, are documented thoroughly.
- **Regular Review of Access Rights:** Granted access rights are regularly reviewed, both periodically and in response to specific events.

3. Protection of IT-Components

3.1 Hardening

- **Unneeded IT components are uninstalled or deactivated**
- **Criticality-Based Component Hardening:** All IT components are protected (hardened) according to their criticality and in alignment with current best practices
- **Restricted Access to Configuration Data:** Access to configuration data and IT component documentation is restricted based on the need-to-know principle.
- **Malware Protection:** Malware Protection is implemented for all IT-components, e.g. gateways, servers, and IT workstations

- **Vulnerability Checks:** IT-Components must be regularly checked for vulnerabilities.
- **Automated Session Termination:** Authenticated sessions are automatically revoked after a reasonable amount of inactivity
- **Protection of Information on Output Devices**

3.2 Asset Management

- **Asset Inventory and Determination of Accountability**
- **Patch Management is in Place**
- **Life Cycle Management is in place**
- **End-of-Life Component Management is In place**
- **Documentation of External Service Maintenance Work**
- **Verification of Component Functionality after Maintenance work**

3.3 Back-Up

- **Backup Concepts are established for IT-Components**
- **Regular Restoration Testing:** Restoration tests are carried out regularly and based on risk, including after procedural or system changes.

4. Network Protection

- **Network Documentation:** The physical and logical structures of the network are documented comprehensively, including spatial arrangement, segmentation, and addressing of network components and segments.
- **Network components operate in access-controlled areas**
- **Network Segmentation:** The network is divided into segments based on protection needs.
- **Data Exchange Security:** Dedicated transition points with access control and packet filtering are implemented, with firewalls configured to allow only authorized data exchanges.
- **Rule Change Verification:** Changes to network access rules are verified.
- **Secure Administration Pathways:** Administration of networks occurs over secure pathways.
- **Remote Access Management:** Remote access is limited to organization-approved IT equipment, requiring two-factor authentication and encrypted communications per cryptographic policies.
- **Secure Communications:** Mechanisms are in place to protect communications between trusted and untrusted networks, using secure channels and mutual authentication for site-to-site connections.
- **Vulnerability Checks:** Network transitions, regulated with firewalls, are regularly checked, especially following significant topology changes.

5. Cryptography

- **Defined usage of Cryptography**: Sensitive data is being encrypted using appropriate methods based on risk.
- **Usage Requirements:** Specified criteria for the selection of method and internal usage are established.

- **Key Management lifecycle:** Comprehensive processes for managing the entire key lifecycle are established.
- **Product Selection:** Cryptographic products are implemented and utilized according to a defined set of specifications.

6. Authentication

- **Password Complexity Requirements**
- **Privileged Access Authentication Requirements:** An appropriate and strong authentication method is used when selecting an authentication mechanism for privileged access, including multi-factor authentication.
- **Regular Mandatory Password Change**
- **Secure Password Storage and Centralized Management:** Passwords for systems and automatic access are securely stored, utilizing centralized management systems with encryption and access logging.
- **SSH Key Management**

7. Logging and Monitoring

- **IT-System Monitoring:** Continuous monitoring of IT systems, applications, and network components is conducted to track security incidents and enable forensic analysis.
- **Integrity Protection Logging and Monitoring Data:** Logging and monitoring data are secured against unauthorized changes and access, with controls in place to prevent unauthorized logging alterations, such as by separating roles that involve administrative functions.
- **Regular Assessments:** Collected logging and monitoring data is subject to regular assessments, conducted at scheduled intervals and upon significant events or incidents.
- **Input Control:** Input actions are logged.

8. Data Transfer Control

- **Authorization and Verification of Recipients**
- **Use of Approved Communication Systems for Business Communication**
- **End-to-end encryption, such as PGP or S/MIME, for Information Transmission**
- **Documentation of Physical Handover of Information**
- **Approval Process for Information Transmission and Disclosure**

9. Protection of Mobile Storage Media and Physical Documents

- **Protected Environment:** All mobile storage devices, such as USB sticks, notebooks, tablets, and CDs/DVDs, and physical documents are kept in a safe and protected environment, like an access-controlled space or lockable cabinet.
- **Encryption of Mobile Storage Devices**

- **Restrictive Policy on the Private Use of Mobile Storage Media**
- **Remote Deletion Capability of Mobile Devices**
- **Clean Desk Policy**

10. Development and Choice of Software

- **Design and Planning:** Risk assessments are conducted, and secure architectures are defined, ensuring chosen technologies satisfy security requirements in software development.
- **Secure Infrastructure and Environment:** Separation between development, test and production environments is maintained with strong access controls in place to safeguard development resources and source code from unauthorized access.
- **Testing and Quality Assurance:** Security testing is integrated into the QA process, with robust error handling developed to effectively manage application failures and vulnerabilities.
- **Privacy by Design:** Privacy standards are implemented throughout the software Development process.
- **Software Approval Process:** All new privacy-relevant software goes through a structured software approval process to ensure compliance with privacy and security standards.

11. Deletion

- **Secure Deletion:** Secure deletion practices ensure permanent data removal through methods such as overwriting or cryptographic erasure for electronic media, and shredding for paper documents, with the destruction process being monitored and documented.

12. Business Continuity Management

- **Risk Analysis and Impact Assessment:** Regular risk analysis and structured Business Impact Analyses are conducted to identify threats and assess the impact on critical business processes, guiding continuity strategies.
- **Continuity Plan Development and Documentation:** Continuity plans are created and regularly updated for all critical processes.
- **BCM Organisation:** Defined roles within the Business Continuity Management System are established to ensure effective strategy execution.
- **Testing and Improving Continuity Plans:** Routine exercises are conducted to test and improve the effectiveness of continuity plans, ensuring ongoing monitoring and continuous improvement in organizational readiness.

13. Data Processor Control

- **Data Processor Selection Based on Due Diligence with a Focus on Data Privacy and Security**
- **Conclusion of Necessary Data Processing Agreements and Provision of Appropriate Guarantees, Including Conduct of Transfer Impact Assessments (TIAs)**
- **Periodic Reviews of Processors' Security Practices**

14. Awareness of Employees

- **Confidentiality Agreements and Security Briefing:** Employees must sign a Confidentiality Agreement and are briefed on information security and privacy during the hiring process.
- **Mandatory Regular Training:** All employees complete initial and regular training sessions, including the topics Privacy and Information Security, which must be completed regularly.
- **Role-Specific Security Training:** Employees receive training specific to the security aspects of their responsibilities, with updates provided when changes occur.

15. Organization and Management

- **Privacy Organization and Role Definition:** Privacy roles and responsibilities are delineated within the organization, ensuring compliance with data protection regulations at all operational levels.
- **Incident Response Management:** An incident response process is in place, integrating privacy considerations to efficiently address and mitigate potential breaches.
- **ISO 27001 Information Security Management:** The organization implements an Information Security Management System (ISMS) aligned with ISO 27001.
- **Security Risk Management:** A risk management, designed to identify, analyze, and manage threats is implemented.
- **Change Management:** A process is implemented to manage changes, ensuring critical assessments and proper documentation are conducted. Rollback measures are maintained for certain changes.
- **Regular Internal Audits**: Internal audits of information security and privacy practices are conducted regularly.