Compeas

Compliance Made Easy

Information security and data protection

White Paper

2026

TABLE OF CONTENTS

Introduction

As technology continues to evolve, organisations face an increasingly complex security landscape shaped by artificial intelligence, digital transformation, and geopolitical developments. While modern technologies introduce new opportunities, they also create new risks. At the same time, the human factor remains one of the most important considerations in maintaining effective information security.

- **The Cloud:** Modern cloud infrastructure provides greater resilience, availability, and recoverability than many traditional on-premises environments. Compeas is built exclusively on European cloud infrastructure and partners with EU-based providers to support GDPR compliance, European data sovereignty, and the secure processing of customer data.
- **Governance, Risk and Compliance:** Governance, Risk and Compliance (GRC) can be complex, particularly for organisations operating across multiple jurisdictions or within regulated industries. Compeas is designed to simplify compliance by helping organisations prepare for, achieve, and maintain compliance with recognised frameworks and regulations, including ISO/IEC 27001, the NIS2 Directive, GDPR, DORA, and the EU AI Act.
- **Our Security Philosophy:** At Compeas, we believe organisations should be able to focus on their core business while maintaining a strong security and compliance posture. Transparency is a fundamental principle of our platform. To support independent assurance activities, Compeas provides dedicated auditor capabilities that enable auditors to access relevant compliance evidence without requiring direct access to customer infrastructure or production systems.
- **Our Commitment to Customers:** Security, privacy, and transparency are fundamental to everything we do. This white paper provides an overview of Compeas' security architecture, operational controls, and data protection practices. If you have any questions or require additional information, we are always happy to assist and provide further guidance.

  - Martin Karlsson, CEO

CHAPTER 1

Our company and products

Compeas is built from the ground up using the latest technology and encryption standards. We believe that AI should be used as a tool but never a decision maker which is why we have built intuitive workflows and interfaces rather than using AI within the product itself.

The company

Compeas was founded in 2026 with the aim to become the leading GRC-platform within Europe. It should be easy for anyone to use Compeas in order to visualise risks, overall compliance, applications, vendors and assets - Martin Karlsson, founder.

Compeas GRC

Compeas GRC is the core of our information security ecosystem, providing a complete ISMS and GRC solution that helps customers manage, monitor, and visualise their security and compliance efforts.

The products

Compeas products are offered as a Software-as-a-Service (SaaS) solution and are accessible via the internet on a wide range of devices. For the optimal user experience, we recommend using a desktop or laptop computer

The auditor tool

The Compeas Auditor Tool is designed for larger organisations and external auditors, providing real-time visibility into compliance progress, evidence, and security activities across multiple Compeas products

Remember you will always find the latest information about our products at our website

CHAPTER 2

Compliance

Data handling

Data handling and GDPR compliance are crucial not only from a legal perspective, but also for maintaining customer trust and confidence, which is why Compeas are committed to maintain the highest standards.

The CEO (former CISO and security professional) is responsible for coordinating and reviewing the security efforts within Compeas and its suppliers, and for ensuring that security standards are followed throughout the organisation.The CEO work together with the CPTO in order to make sure that the entire development process and product features are built with security and privacy in mind.

GDPR

The General Data Protection Regulation (GDPR) is one of the most important pieces of legislation governing the protection of personal data, ensuring that organisations handle customer information, including personally identifiable information (PII), in a lawful and responsible manner.

Compeas is designed with GDPR compliance as a core principle. Each customer is provided with a dedicated database, helping to minimise the risk of data leakage and prevent unauthorised access or misuse of PII. In addition, our products are built to support data portability, enabling customers to easily export their data when required.

To reinforce this commitment, all employees are required to complete mandatory GDPR training as part of their ongoing security and compliance programme.

Standards

The Compeas ISMS is aligned with ISO/IEC 27001:2022, with controls applied on a risk-based applicability basis as documented in our Statement of Applicability. We are working towards ISO/IEC 27001 certification, planned for 2027. We have a risk-based approach in everything we do. Our development process follows OWASP Top 10 and NIST SP 800-53.

CHAPTER 3

Security and awareness

At Compeas, we conduct continuous security awareness training and regular awareness sessions for all employees to ensure a strong and sustained security culture across the organisation. We also ensure that every employee is required to read and acknowledge the applicable information security policies and adhere to established security best practices using the Compeas GRC platform.

Our security programme, including mandatory GDPR training, applies to all employees and consultants without exception. All policies and security standards are reviewed and updated on at least an annual basis to ensure they remain current, effective, and aligned with relevant regulatory and organisational requirements.

Upon joining Compeas, every new employee is enrolled into the Compeas GRC platform and assigned the required training curriculum as part of their onboarding process. Before access to any internal systems is granted, the employee must successfully complete the mandatory baseline security awareness training.

Phishing simulation

As part of our continuous security training efforts, Compeas conducts recurring phishing simulations to strengthen employee awareness and reinforce secure behaviour.

Security training

Compeas places a strong emphasis on continuous security education and awareness across the organisation. Employees and consultants regularly participate in security training sessions and information security seminars designed to increase awareness of current threats, industry best practices, and evolving regulatory requirements.

These training initiatives cover topics such as phishing and social engineering, password security, secure data handling, GDPR compliance, incident reporting, and general cybersecurity best practices. By providing ongoing education and practical awareness activities, Compeas aims to foster a strong security culture and ensure that all personnel understand their role in protecting customer data and maintaining the organisation's security standards.

CHAPTER 4

Security and Privacy Commitments

Data processing and sub-processors

Compeas processes customer data in accordance with applicable data protection legislation, including the General Data Protection Regulation (GDPR). Data processing activities are governed by Compeas' Data Processing Agreement (DPA), which forms part of the contractual relationship with each customer.

Compeas maintains a publicly available register of authorised sub-processors used in the delivery of the Compeas platform. The register is continuously maintained to ensure customers have access to the most current information regarding active sub-processors and the services they provide. The current list is available at: **compeas.com/trust-centre/subprocessors**

Security incident notification

Compeas maintains documented procedures for detecting, assessing, responding to, and recovering from security incidents. Where a confirmed security incident affects customer data or services, affected customers will be notified without undue delay in accordance with applicable law and the contractual notification requirements defined in the Service Agreement and Data Processing Agreement.

Data return and secure deletion

Upon termination of the service, customers may request the return of their customer data in accordance with the terms of the Master Subscription and Services Agreement (MSSA). Following the applicable retention period and unless otherwise required by law or agreed in writing, customer data is securely deleted from production systems and backup media in accordance with Compeas' data retention and secure disposal procedures.

CHAPTER 5

Customer & application security

Customer data security

Access to customer data and production infrastructure is governed by the principle of least privilege. Only authorised personnel whose job responsibilities require such access are granted access to production systems, customer environments, or infrastructure components.

Access is provided on a need-to-know basis and is restricted through role-based access controls, approval workflows, and authentication requirements. All privileged access is traceable, monitored, and regularly reviewed to ensure that permissions remain appropriate and aligned with current responsibilities.

Access to customer data is limited to specific operational purposes such as system maintenance, troubleshooting, support, or security-related activities, and is only granted for the minimum level and duration required to perform the task.

Application security

Access to the application and its associated data at Compeas is secured through unique personal identities managed via trusted identity providers. SSO and MFA integrations are configured on the customer side with the customer's own identity provider. Compeas does not itself use any non-EU service providers. Authentication is enforced using SSO combined with multi-factor authentication (MFA), including Microsoft or Google Authenticator, to ensure a strong and secure login process for all users.

Passwords and other sensitive authentication data are stored in encrypted form, following industry best practices to protect against unauthorised access. Where applicable, password policies enforce sufficient complexity and length requirements to further strengthen account security.

Access to customer data is strictly controlled through role-based access control (RBAC) and the principle of least privilege, ensuring that users can only access the data and functionality required to perform their specific job responsibilities. Server-side authorisation mechanisms validate all access requests, ensuring that only permitted data is transmitted to the client layer and preventing unauthorised data exposure.

Access to full datasets and administrative functionality is limited to authorised Compeas personnel who require such access for operational purposes, such as support, maintenance, or troubleshooting. This access is regularly reviewed and adjusted based on current business needs.

All Compeas personnel are bound by confidentiality obligations and receive security training as part of their onboarding and ongoing awareness programme. In addition, all communication between clients, services, and third-party systems is encrypted using industry-standard encryption protocols to ensure the confidentiality and integrity of data in transit.

Database security

Data stored within Compeas infrastructure is protected using encryption at rest and industry-standard security controls provided by our hosting provider. Sensitive data and storage systems are safeguarded through secure key management mechanisms designed to protect against unauthorised access and data exposure.

To further strengthen customer data protection, each customer is provisioned with a dedicated database instance. Compeas does not rely solely on logical separation within shared databases; instead, customer environments are segregated at the database level to reduce the risk of cross-customer data exposure and minimise the impact of potential security incidents or data leaks.

Development, testing, staging, and production environments are separated across dedicated servers and network segments, with strict access controls applied between environments. All environments are maintained according to security standards aligned with production-level security practices to ensure consistent protection throughout the development lifecycle.

Changes to critical application data, administrative actions, access rights, and other security-relevant events are logged and monitored to support traceability, auditing, and incident investigation. Logging applies both to actions performed by authorised Compeas personnel and by customer users within the platform.

In addition, Compeas continuously reviews and monitors its infrastructure and security controls to maintain a high level of data protection, integrity, and operational security across all customer environments.

CHAPTER 6

Platform security

Compeas hosting environment is designed as a secure, redundant, and scalable cloud infrastructure hosted within Ploi Cloud's EU-based data centres.

Data centre security

Compeas hosts its platform infrastructure within the European Union to support GDPR compliance and European data sovereignty requirements. The Compeas platform is hosted in Sweden using Ploi Cloud's infrastructure platform, which operates on UpCloud infrastructure hosted within the Equinix Stockholm SK2 data centre. The facility provides enterprise-grade physical security, resilient infrastructure, and is certified according to internationally recognised security standards, including ISO/IEC 27001.

Compeas complements the underlying infrastructure security controls with its own application security, access management, monitoring, backup, and operational security measures. Together, these controls are designed to protect the confidentiality, integrity, availability, and traceability of customer data and services.

More information regarding Equinix Stockholm SK2's physical security, infrastructure controls, and certifications can be found in Equinix's data centre documentation (here).

Platform hardening

Compeas continuously monitors security advisories, vulnerability disclosures, and vendor updates relevant to our infrastructure and technology stack. Security updates and patches are evaluated based on risk, severity, and impact to Compeas and its customers before deployment into production environments.

Our infrastructure is built on hardened Linux-based operating systems configured according to security best practices and the principle of least functionality. Unnecessary services, ports, and software components are disabled or removed to minimise the attack surface and strengthen overall system security.

In addition, Compeas applies ongoing system maintenance, security monitoring, and configuration management procedures to ensure that servers and infrastructure components remain secure, stable, and up to date.

CHAPTER 7

Encryption

All communication between users, customer environments, internal services, and third-party integrations within Compeas platform is protected using modern industry-standard encryption protocols. Compeas utilises **TLS 1.2+/1.3** to secure all data transmitted between clients and backend services, ensuring strong protection of data in transit while aligning with modern cryptographic best practices and post-quantum encryption readiness initiatives.

Authentication and security-related operations utilise secure cryptographic mechanisms and hashing algorithms designed to protect sensitive information against unauthorised access and credential compromise. Passwords and authentication secrets are never stored in plain text and are instead protected using **Argon2id** hashing, recognised as one of the leading password hashing standards for secure credential storage.

Compeas also utilises **SHA-256** cryptographic functions in combination with **2048-bit RSA**-based security mechanisms to support secure authentication, integrity validation, and cryptographic operations across the platform. These controls help ensure the confidentiality, integrity, and authenticity of sensitive data and system communications.

In addition, Compeas applies secure token-based authentication mechanisms and encryption controls across both transport and storage layers to ensure that customer data remains protected throughout its lifecycle, including during transmission, processing, and storage within Compeas infrastructure.

CHAPTER 8

Disaster recovery, backups and continuity

Compeas infrastructure is hosted within Ploi Cloud's EU infrastructure environment, using the Stockholm (SE-STO1) location operated on UpCloud infrastructure and hosted at the Equinix Stockholm SK2 data centre. The platform is designed with redundancy and operational resilience measures to support high availability and service continuity.

In the unlikely event of a major outage or failure affecting the primary hosting environment, Compeas maintains documented business continuity and disaster recovery procedures designed to restore critical services and customer operations as quickly as possible. Recovery objectives, including Recovery Time Objective (RTO) and Recovery Point Objective (RPO), are defined and managed according to Compeas' Service Level Agreement (SLA).

Compeas' business continuity and disaster recovery processes are regularly reviewed, tested, and updated as part of its ongoing operational resilience and information security programme.

Backups

Compeas performs automated backups of critical systems, application configurations, and customer data to support data availability and operational resilience. Backups are securely stored across separate storage locations and replicated to secondary infrastructure environments to reduce the risk of data loss in the event of infrastructure failure or disaster scenarios.

In addition to scheduled backups, critical data is replicated between environments to support recovery operations and minimise potential service interruption. This approach supports Compeas' Recovery Point Objective (RPO) of approximately 1–3 hours and helps ensure that customer data can be restored with minimal data loss in the unlikely event of a major incident.

Backup integrity, retention, and recovery procedures are regularly monitored and reviewed as part of Compeas' disaster recovery and business continuity programme. Backups are retained according to internal retention policies and operational requirements to support recovery operations and applicable data protection obligations.

CHAPTER 9

Support and Availability

Service availability & Support

Compeas provides a highly available and scalable SaaS platform designed to ensure stable and reliable service delivery for customers. The infrastructure is built with redundancy, failover capabilities, and continuous monitoring to minimise downtime and maintain operational continuity.

Service availability is continuously monitored, and planned maintenance activities are scheduled and communicated in advance whenever possible to minimise customer impact. Compeas maintains operational procedures and incident management processes designed to quickly identify, manage, and resolve service-related incidents.

Customer support is available during standard business hours, Monday to Friday, 09:00–17:00 CET (Stockholm time). All support requests and incidents are logged, tracked, and managed through Compeas support and ticket management processes to ensure proper handling, traceability, and resolution.

To protect customer data and maintain security, only authorised customer representatives may request changes or receive access to customer-specific information. Access to customer environments and data by Compeas personnel is governed by strict access control procedures and the principle of least privilege.

Support and operational matters are handled collaboratively between relevant operational, technical, and development teams depending on the nature and complexity of the issue, ensuring that incidents and requests are managed by the appropriate personnel.

www.compeas.com

info@compeas.com

linkedin.com/company/compeas

Scan the QR code below to get straight to our webpage:

Important Notice

This document is provided for informational purposes only and does not constitute a contractual commitment. The security controls, processes, and technical measures described in this white paper are subject to continuous improvement and may change over time. Contractual commitments are governed exclusively by the applicable Master Subscription and Services Agreement (MSSA), Data Processing Agreement (DPA), and Service Level Agreement (SLA).

Compeas

Compliance Made Easy