Compeas

Compliance Made Easy



Information security and data protection

White Paper

2026

TABLE OF CONTENTS

Introduction	3
Our company and products	4
Governance and compliance	5
People and awareness	6
Privacy commitments	7
Application security	8–9
Hosting and infrastructure	10
Encryption	11
Backups and continuity	12
Secure development and vulnerabilities	13
Support, availability and the Trust Center	14

Introduction

Organisations depend on more suppliers, more cloud services and more regulation than ever. A supplier that holds compliance records must show, not merely state, how it protects them.



- **Customer data in the EU.** Compeas GRC runs on European cloud infrastructure: the application and its database in Amsterdam, the Netherlands, and uploaded files in Stockholm, Sweden. Each customer has its own installation, with its own database, storage buckets and encryption key.
- **Governance, risk and compliance made manageable.** Compeas helps organisations prepare for, achieve and keep compliance with frameworks and regulations such as ISO/IEC 27001, NIS2, the GDPR, the Cyber Resilience Act, ISO 9001, ISO 14001, SOC 2 and the NIST Cybersecurity Framework.
- **Transparency by design.** Auditors work from the evidence in the platform rather than from screenshots, and the Compeas Trust Center shows publicly which security controls Compeas has proven, kept current from Compeas GRC.
- **The same rules for Compeas itself.** Compeas runs its own information security management system in Compeas GRC, against ISO/IEC 27001:2022 and the GDPR.

This white paper describes the measures Compeas has in place today: how the platform is built and hosted, how data is protected, and how security work is organised. Where a measure is still being put in place, the text says so. Questions are welcome at **security@compeas.com**.

Martin Karlsson, CEO

CHAPTER 1

Our company and products

AI is a tool, never a decision maker. Compeas GRC guides people through clear workflows, and every judgement stays with a person.

The company

Compeas AB is a Swedish company, founded in 2026 and based in Köping, Sweden (organisation number 559590-5703). Its aim is to be the leading GRC platform in Europe, easy enough for anyone to use to see risks, compliance, applications, vendors and assets in one place.

Compeas GRC

The core product: a complete information security management system and GRC platform in which customers manage, monitor and prove their security and compliance work. It is offered as Software as a Service and used in a web browser.

The Compeas Auditor Tool

For groups of companies and for external auditors: a view of compliance progress, evidence and security work across several Compeas GRC installations. Each company decides what the Auditor Tool may read by issuing its own expiring API keys.

The Compeas Trust Center

A public page on which an organisation shows what it has proven: badges, controls in place, sub-processors, the personal data it processes and documents on request. It is kept current from Compeas GRC, and a control appears only once its proof is approved. Compeas publishes its own at trust.compeas.com.

Artificial intelligence

Compeas GRC runs no AI models of its own and makes no calls to AI services. A customer may connect its own AI assistant (Claude, ChatGPT or Copilot) to read its compliance record. The connection is off until an administrator turns it on, is read-only, and never sees people's names or email addresses. Chapter 5 describes it.

> The latest information about the products is always at compeas.com.

CHAPTER 2

Governance and compliance

Information security management

Compeas runs its information security management system (ISMS) in Compeas GRC, against ISO/IEC 27001:2022. Its policies, risk assessment, Statement of Applicability, controls, evidence, incidents and internal audits are all kept there. Controls are applied on a risk basis, as the Statement of Applicability records.

ISO/IEC 27001 certification

Compeas is not yet certified. It is preparing for certification by a certification body accredited by Swedac. Until then, the Trust Center lists only the controls whose proof has been approved.

Responsibilities

The CEO, a former CISO, is responsible for information security and privacy at Compeas and among its suppliers, and approves every change to the platform before release. The CEO makes sure that features and the development process are built with security and privacy in mind.

The GDPR

For the personal data in Compeas GRC, the customer is the controller and Compeas the processor. A data processing agreement under Article 28 of the GDPR is part of every customer agreement.

Compeas has assessed Article 37 and is not required to designate a data protection officer; the CEO is the privacy lead and the contact for the Swedish Authority for Privacy Protection (IMY). Compeas processes no special categories of personal data for its own purposes.

Customers can export all their data at any time (data portability), and Compeas assists them with data subject requests and personal data breaches.



CHAPTER 3

People and awareness

Security depends on the people who run the service. Compeas keeps its team small, its access narrow and its rules written down.

Policies everyone accepts

Compeas's information security policies are approved by management and shared with staff in Compeas GRC, where each person reads and accepts them. A person gets access to Compeas systems only after accepting them, and accepts them again when a policy changes in substance. Policies are reviewed at least once a year.

Confidentiality

Everyone who works for Compeas is bound by confidentiality obligations, and the Compeas staff who support customers are bound by obligations at least as protective as those in the customer agreement.

Training

Security awareness and GDPR training is given on joining and at least once a year. It covers phishing and social engineering, passwords and multi-factor authentication, handling of customer and personal data, and how to report an incident.

Developers also receive secure development training at least once a year, covering how to prevent injection, cross-site scripting, cross-site request forgery, broken authorisation, insecure sessions and vulnerable libraries.

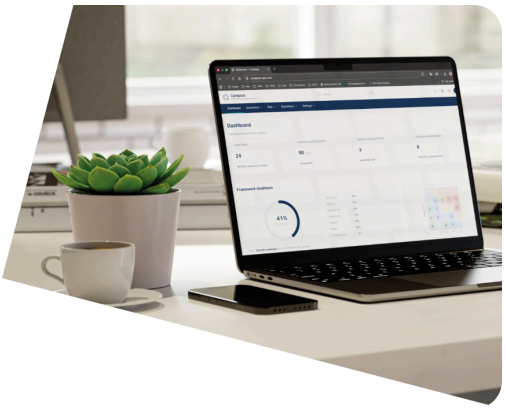
Leaving or changing roles

Access is removed promptly when someone leaves or no longer needs it, and at the latest within 24 business hours.



CHAPTER 4

Privacy commitments



Data processing agreement

The data processing agreement is Annex A to the Compeas Master Subscription and Services Agreement and follows Article 28 of the GDPR. It lists the sub-processors, where each processes data and what for. Customers are told in writing before a new sub-processor is engaged and may object within 30 days. Customers may audit compliance with the agreement.

Where data is processed

Personal data in the platform is processed and stored within the EU/EEA. Published Trust Centers and the sign-in pages run on Cloudflare: their data is stored in the EU, and requests are handled at the Cloudflare data centre nearest the visitor, under the EU–US Data Privacy Framework and standard contractual clauses.

Sub-processors

The current list, with each company's purpose, data location and transfer safeguard, is published at **trust.compeas.com**.

Security incident notification

Customers are notified in writing without undue delay, and in any case within 72 hours, of any confirmed or reasonably suspected incident that affects or is likely to affect their data. The notice describes what happened, the data and people concerned, the likely consequences and the measures taken. Compeas helps customers meet their own duty to notify under Articles 33 and 34 of the GDPR.

Data return and deletion

Customers can export all their data at any time. For 30 days after the contract ends, an export is available on request; the data is then deleted as the data processing agreement sets out, including copies in backups as their retention cycle ends, and Compeas confirms the deletion in writing on request.

CHAPTER 5

Application security

One installation per customer

Each customer has its own installation of Compeas GRC: its own application, its own PostgreSQL database, its own storage buckets and its own encryption key. Customers never share a database, so one customer's data cannot be reached through another customer's account.

Signing in

- Single sign-on with Microsoft Entra ID or Google Workspace, set up per installation. Google sign-in is limited to the customer's own Workspace domain.
- Password sign-in can be turned off once single sign-on works.
- Passwords have at least 12 characters with upper and lower case, numbers and symbols, and are checked against known breached passwords.
- Two-factor authentication with an authenticator app or an emailed code. Administrators and compliance managers must use it; other users can turn it on. A sign-in through an identity provider that has already performed multi-factor authentication counts.
- Repeated failed attempts are throttled, and every sign-in, failed sign-in and lock-out is logged.
- Sessions are encrypted, expire after two hours of inactivity and use secure, HTTP-only cookies.

Roles and authorisation

Access inside the platform follows roles: administrator, compliance manager, control owner, risk manager, risk owner, auditor and user. Every request is authorised on the server, and only the data a role may see is sent to the browser.

Audit log

Every change to a record, and every sign-in, is written to an append-only audit log with the person, time, IP address, the old and new values and, where given, the reason. Secrets are left out of it. Administrators, compliance managers and auditors can read and export it; each export carries a SHA-256 checksum and is itself logged. The audit log is kept for the life of the installation.

Protection in the browser

The platform sends a Content Security Policy with per-request nonces, forbids framing by other sites, requires HTTPS through HSTS, and sends nosniff, referrer and permissions policies. The framework's protections against injection, cross-site scripting and cross-site request forgery are used throughout.

Access by Compeas staff

Only the Compeas staff who run the platform can reach production systems, with multi-factor authentication, and only to operate or support the service. Access is reviewed regularly and logged.

Auditors and the Auditor Tool

An auditor can be given the auditor role inside an installation, or read it from the Compeas Auditor Tool through an API key that the customer issues. API keys are stored only as hashes and must have an expiry date. Personal data, incidents and vulnerabilities are readable only through scopes the customer grants, and a key that reads personal data needs a recorded lawful basis and expires within 12 months.

Data export

Administrators can export every register as a file at any time, or the whole installation as one archive: every register, the audit log, the Statements of Applicability and every stored file, with a manifest of SHA-256 checksums. Passwords, two-factor secrets, API keys and integration tokens are never exported.

AI assistants

A customer may connect its own AI assistant (Claude, ChatGPT or Copilot) to its Compeas GRC installation:

- The connection is off until an administrator turns it on and chooses who may use it.
- The assistant can only read; it cannot change anything.
- It signs in with OAuth 2.1 and PKCE. Access tokens last one hour.
- Names, email addresses, Swedish personal identity numbers and phone numbers are removed from every answer, and data read from Google Workspace is never sent.
- Files and policy texts are never returned.
- Every call is logged in the audit log and limited in rate.

The customer's assistant, not Compeas, processes the answers, under the customer's own agreement with its AI provider.

CHAPTER 6

Hosting and infrastructure

Compeas GRC is hosted in the European Union, in Amsterdam, the Netherlands, and Stockholm, Sweden.

Data centre and platform

Compeas GRC and the Compeas Auditor Tool run on Ploi Cloud, a managed cloud platform that runs on infrastructure from UpCloud, a Finnish cloud provider whose cloud service is certified to ISO/IEC 27001:2022. The application, its database and the nightly backups are in UpCloud's data centre in Amsterdam, the Netherlands. Uploaded files, such as policies, evidence and vendor documents, are stored in Ploi's object storage in Stockholm, Sweden.

Ploi Cloud runs the servers and the container platform. Compeas manages the application, its configuration and its dependencies, and adds its own access control, logging, backups and security testing.

Separate environments

Development takes place with demonstration data. Customer data is not used for development or testing unless the CEO has explicitly approved it. Every customer installation is separate from the development and test environments.

Other services

- **Cloudflare** serves the website, the sign-in pages and published Trust Centers, and provides DNS. Stored data is kept in the EU.
- **AhaSend** delivers the emails the service sends, within the EEA, from noreply@compeas.com.
- **Google Workspace** carries Compeas's business email and support communications.

When a customer connects its own tools, such as Microsoft 365, Google Workspace or Jira, the data in those tools stays in the customer's own accounts. What Compeas GRC reads from them, such as the results of its checks, is kept in the customer's own installation.

Monitoring

The availability of each installation is monitored continuously, and service status is published at status.compeas.com.

CHAPTER 7

Encryption

What is encrypted, how, and where encryption is not applied.

DATA	PROTECTION
All traffic to Compeas GRC	HTTPS with TLS 1.2 or 1.3; older versions are refused. Browsers are told to use HTTPS only (HSTS).
Connections to other services	Encrypted with TLS: Microsoft, Google, Jira, email delivery and file storage.
Secrets in the database	Encrypted by the application with AES-256, using a key unique to each customer's installation: integration tokens, single sign-on secrets, two-factor secrets, signing keys and sessions.
Passwords	Stored only as bcrypt hashes, never in readable form.
API keys and invitation links	Stored only as SHA-256 hashes, so they cannot be read back.
Uploaded files	Encrypted at rest with AES-256 in object storage.
Nightly backups	Encrypted with AES-256-GCM.
Database storage	The storage volumes of the production databases are not encrypted at rest by the hosting provider. Access to them is limited to the staff who run the platform, with multi-factor authentication, and is logged; the secrets in the databases are encrypted by the application, as above.

Keys

Each installation has its own application key, generated when the installation is created; no two customers share one. Only the people and systems that need a key can reach it, and a key is replaced at once if compromise is suspected. The storage and backup providers manage the keys for the encryption they apply.



CHAPTER 8

Backups and continuity

Nightly	24 h	4 h	99.7%
automatic backup of each installation's database	recovery point objective (RPO)	recovery time objective (RTO)	monthly availability target

Backups

Each installation's database is backed up automatically every night, encrypted with AES-256-GCM. Backups are kept in the hosting provider's backup storage, separate from the application and the database, in the EU.

The recovery point objective is 24 hours and the recovery time objective 4 hours, as the customer agreement sets out.

Business continuity and disaster recovery

Compeas keeps a documented business continuity and disaster recovery plan for restoring the service and customer data after a major disruption, and reviews it at least once a year.

Restoring an installation from backup is tested at least once a year, and each test is recorded in Compeas GRC.

CHAPTER 9

Secure development and vulnerabilities

Every change reviewed

All Compeas code is kept in private GitHub repositories. Every change is made on its own branch and reaches the main branch only through a pull request. Before a change is merged:

- the full automated test suite, more than 4,000 tests, has passed;
- a written security review in the pull request covers the data, access, input and output, third parties and AI exposure the change touches;
- the CEO has approved it.

The pull request keeps the record of each change, its review and its tests.

Penetration testing

The platform is penetration tested at least once a year and after material changes to the hosting architecture or security controls. The latest test, in November 2026, was an internal test with full access to the source code, covering the application, the public API, the AI connection and the Auditor Tool. It found no critical or high-risk vulnerabilities, and its findings are remediated within the targets below.

Finding vulnerabilities

Compeas follows CERT-SE, CISA's catalogue of known exploited vulnerabilities, the security bulletins of its main suppliers and the Dependabot alerts on its code repositories. The findings are reviewed at least monthly, and each review is recorded in Compeas GRC with the action decided.

Fixing them

SEVERITY	REMEDIATED WITHIN
Critical	30 days
High	30 days
Medium	60 days
Low	90 days

Reporting a vulnerability

By email to security@compeas.com, in English or Swedish. Reports are acknowledged within 48 hours. The contact and the disclosure policy are also published at compeas.com/.well-known/security.txt, with a PGP key for encrypted reports.

CHAPTER 10

Support, availability and the Trust Center

Availability

Compeas GRC and the Compeas Auditor Tool each have an availability target of 99.7% per calendar month, with service credits when it is not met. Scheduled maintenance that affects availability is announced at least five business days in advance.

Support

Support is available Monday to Friday, 09:00–17:00 Swedish time, by email to support@compeas.com, by phone on +46 10 265 00 70 and through compeas.com/contact. Critical incidents are handled around the clock.

PRIORITY	FIRST RESPONSE
1 Critical	Within 30 minutes, every day
2 High	Within 2 hours
3 Medium	Within 1 business day
4 Low	Within 2 business days

Only authorised customer representatives may request changes or receive customer-specific information.

The Compeas Trust Center

At **trust.compeas.com**, Compeas publishes the security controls it has proven, its sub-processors, the personal data it processes and answers to common questions. It is kept current from Compeas GRC.

The data processing agreement and the service level agreement can be downloaded there. Policies and other documents can be requested; access is granted for a limited time under a non-disclosure agreement, and every downloaded PDF is marked with the recipient's email address.

Contacts

- Security: security@compeas.com
- Data privacy: privacy@compeas.com
- Support: support@compeas.com



www.compeas.com

info@compeas.com

trust.compeas.com

linkedin.com/company/compeas

Scan the QR code to go straight to compeas.com:

Compeas

Compliance Made Easy

Important notice

This document is provided for information only and is not a contractual commitment. The security controls, processes and technical measures it describes are improved continuously and may change. Contractual commitments are set out only in the applicable Master Subscription and Services Agreement, Data Processing Agreement and Service Level Agreement.

Version 2.0, November 2026. Copyright © 2026 Compeas AB. All rights reserved.

Compeas

Compliance Made Easy