NEOWHISTLE

Security & privacy whitepaper

SEPTEMBER 2026

ISSUED BY

BELFORTADVISORY

1. Introduction

When an individual decides to blow the whistle, potential extremely sensitive information is being disclosed. It's vital to the whistleblower that their personal data is properly secured. Likewise, it is of great importance to the organization and its trusted persons that the report is adequately secured. To comply with the EU directive on whistleblowing and the national legislation as well as the GDPR, each organization that is subject to it should assess carefully which information technology solution they should implement.

2. Purpose

The purpose of this document is to inform the reader about the processes that the Neo Whistle team adheres to, as well as the technical control measures that are applied to the Neo Whistle SaaS solution, with the goal of maximizing security and privacy and minimizing the associated risks.

3. Processes

3.1 Human Resource processes

Background checks are performed prior to hiring new employees/contractors. Upon employment/contracting, they are required to sign a Non-Disclosure Agreement.

Neo Whistle is operated by whistlebox, a company under Belgian law which only employs employees and contractors in Belgium.

3.2 IT processes

3.2.1 Incident response

Neo Whistle has an Incident Response Plan to address service availability, integrity, security, privacy, and confidentiality issues. This plan details the roles and responsibilities that all involved parties adhere to during the lifetime of an incident. An incident management tool is used to ensure the necessary information about incidents is documented, and corrective actions are taken.

3.2.2 Disaster recovery

The Disaster Recovery Plan (DRP) enables Neo Whistle to resume normal operations after a disaster. The DRP is tested yearly. Encrypted backups are performed on a regular basis

and stored within the European Union, and restore procedures are validated as part of the yearly DRP test.

3.2.3 Business continuity

Neo Whistle has set up a Business Continuity Plan (BCP) to address how to resume or continue providing services to users, as well as how to function as a company, if business-critical processes and activities are disrupted.

3.2.4 Privacy by design

When designing the application and all significant changes to its functionality, the Neo Whistle team puts privacy and security first.

3.2.5 Security & privacy review meeting

Every 6 months, Neo Whistle holds a security & privacy review meeting, where multi-disciplinary participants discuss incidents, assess risks and take actions to improve.

3.2.6 Data retention

Neo Whistle processes customer data solely as a data processor on behalf of the customer. Report data is retained only as long as necessary for the purposes for which it is processed and is retained or deleted in accordance with the customer's instructions and applicable whistleblowing and data protection legislation. Upon termination of the service, or at the customer's request, customer data is securely deleted.

4. Third-party sub-processors

Our third-party sub-processors are:

- whistlebox, whistleblowing platform operator, based in Belgium
- OVHcloud, cloud hosting provider headquartered in France, with hosting for this service in Germany
- Rapidmail, email delivery service based in Germany
- FriendlyCaptcha, captcha provider based in Germany

By using European sub-processors, Neo Whistle safeguards digital sovereignty: data is processed only in the EU and remains under European jurisdiction, without exposure to extraterritorial legislation from outside the EU.

5. Application security

5.1 Security audits

The application is subjected yearly to penetration tests from a specialised third party. Neo Whistle maintains an information security program aligned with ISO 27001 controls; Neo Whistle is not itself certified to ISO 27001 at this time.

Source code is scanned for possible security vulnerabilities before deployment to production.

5.1.1 Responsible disclosure

Neo Whistle welcomes the responsible disclosure of suspected security vulnerabilities. Suspected issues can be reported to neo@belfort-advisory.com and are triaged and remediated according to their severity.

5.2 Hosting

The application is hosted in European data centres of OVHcloud, the largest European cloud provider, headquartered in Roubaix, France. The application runs in OVHcloud's Frankfurt data centre in Germany. More info on this page: https://www.ovhcloud.com/en/about-us/

All OVHcloud services hosted in European data centres have certifications for the following relevant standards:

- ISO-27001 (Information Security)
- ISO-27017 (Cloud Security)
- ISO-27018 (Cloud Privacy and Data Protection)
- ISO-27701 (Privacy Information Management)

More info about the certifications on this page:
https://www.ovhcloud.com/en/enterprise/certification-conformity/

The OVHcloud Security Policy can be found here: https://docs.ovh.com/gb/en/security/issp/

5.3 Application architecture

The application architecture is designed and built from the ground up as a secure messaging system. Security and encryption are at its core.

5.3.1 Keystores

Each user has exactly one keystore. A keystore contains both public and private keys of resources (reports, messages, users) the user has access to.

- Keys are derived from the secp256k1 EC using a secure random function.
- Each keystore contains one set of master keys. These are the user's personal public and private key.
- Public keys are never encrypted.
- Private keys are always encrypted.
- The private master key is symmetrically encrypted using a stretched hash of the user's passphrase (which is subject to a strict password policy).
- All other private keys are encrypted asymmetrically using the user's public and private keys (also includes HMAC-SHA1 signing).
- Symmetric encryption scheme is AES-256.
- Users are unable to access theirs or anyone else's keystore directly.
- Keystore sessions are short-lived.

5.3.2 Secure content

Databases are encrypted using LUKS (Linux Unified Key Setup) to ensure security for all data at-rest. The unique encryption key is managed by OVHcloud. On top of this database encryption, all conversations and attachments within the application are encrypted and signed using an elliptic curve integrated encryption scheme (ECIES), where only the users in the conversation (reporter & confidential advisors) have the key (derived from their password – see above) and thus the possibility to access the content. Neo Whistle and its subcontractors do not have the possibility to access the conversation content in any circumstance.

The application has a layered design that retains strict domains and responsibilities. Customer data is stored in a separate database instance from other clients.

5.3.3 Encryption in transit

All data exchanged between users and the application is encrypted in transit using TLS 1.2 or higher, and connections are served exclusively over HTTPS.

5.3.4 Authentication

Neo Whistle uses keystores in conjunction with a customised OAuth2/OpenID Identity Provider. This merger results in a secure system that does not store password hashes.

Case handlers are required to set up two-factor authentication via access codes that adhere to the TOTP (Time-based One-Time Passwords) algorithm standard.

5.3.5 Authorization

The application employs basic role-based access that is integrated by design.

5.3.6 Internal access to data

Access to production systems is restricted to authorised personnel on a need-to-know and least-privilege basis, is individually attributable, and is logged. As set out under Secure content, conversation content is encrypted such that Neo Whistle and its subcontractors cannot access it under any circumstance.

5.3.7 Anonymity

Reporters can choose to report anonymously. The Neo Whistle solution does not log IP addresses and metadata are stripped from attachments.

5.3.8 Anti-virus scans

Every file that is uploaded by the users of the application is scanned for trojans, viruses, malware & other malicious threats. The virus scan database is kept up to date.

5.3.9 Audit trail

All reports have an immutable, tamper-proof audit trail of all changes applied to it (new message, user added, updated metadata, etc.).