NEOWHISTLE

Whistleblowing reporting channel

SPEC SHEET - SEPTEMBER 2026

ISSUED BY

BELFORTADVISORY

1. What?

- Neo Whistle is a ready-to-use reporting channel with a full case management back office, built to meet European Directive 2019/1937, better known as the whistleblowing directive, and the national laws that transpose it across the EU member states.
- The directive requires organisations to provide an internal reporting channel, so that employees, and optionally external reporters, can safely report wrongdoing to the case handlers, the confidential advisers appointed by the organisation.
- Those case handlers can be the organisation's own people, for example an HR officer or a compliance officer, or an external party handling cases on the organisation's behalf.
- The directive offers a robust framework for whistleblowing that also serves as a strong foundation for organisations outside the EU.
- The text on every reporter-facing screen can be adapted to the organisation's own wording, so the channel speaks the language of the organisation and not of the software.

2. How?

- The channel is set up automatically for each organisation, and activation emails are sent to the case handlers.
- Reporters raise a concern through a secure channel and stay in contact with the case handler in a user-friendly chat style conversation.
- Reporters choose whether to report anonymously or with their identity. Two-way messaging works either way.
- Reporters create their own login details and receive a case ID, which supports their protection against retaliation.
- Case handlers work the case in the back office, with a dashboard, filters and statistics, and can discuss among themselves at case level.
- Access is granted per case, so only the people who need to see a report can see it. External consultants can be given access to a single case.
- All communication stays inside the secure environment. Nothing sensitive travels by email.
- Closed cases can be archived. Personal data is purged while anonymised statistics are kept.

3. Specs

3.1 The reporting channel

- Ready to use, nothing to install
- Anonymous or identified reporting, as the reporter chooses
- Encrypted two-way messaging, also with anonymous reporters
- Available in 17 languages, with more added over time
- Works on computer, smartphone and tablet
- Email notifications when there is new activity on a case

3.2 Case management

- Intuitive case management back office
- Case dashboard with filters
- Statistics on reports

© Neo Whistle | Belfort Advisory

- Individual access management per case
- Access for external consultants
- Secure internal chat between case handlers
- Case archive that purges personal data and keeps anonymised statistics
- An administrating case handler can correct or remove reported content, so GDPR requests can be honoured
- Unlimited number of cases and case handlers

3.3 Configuration per channel

- The text on virtually every reporter-facing screen
- The logo and the homepage image shown on the channel
- Anonymous reporting allowed or not
- Anonymous or confidential reporting as the default
- The qualifications (categories) a report can be filed under
- The input fields the reporter fills in
- The privacy notice text
- Optional FAQ and About us pages
- Colours, favicon, email templates and the domain are set once by the provider of the channel and apply to every channel it operates

3.4 Security and data protection

- End-to-end encrypted conversations and attachments. Only the reporter and the case handlers on the case hold the keys, so neither Neo Whistle nor its subcontractors can read the content
- Each customer's data in a separate, encrypted database instance
- Encrypted in transit over HTTPS at all times
- Mandatory two-factor authentication for case handlers
- No IP addresses logged, and metadata stripped from uploaded files, so anonymous stays anonymous
- Every uploaded file scanned for viruses and malware
- Immutable, tamper-proof audit trail on every report
- Yearly penetration test by a specialised third party
- Information security programme aligned with ISO 27001 controls. Neo Whistle is not itself ISO 27001 certified
- The security and privacy white paper sets out the full technical and organisational detail, and is available on request

3.5 European by design

- All data is processed inside the European Union, on infrastructure operated by European providers only
- No providers from outside the EU are used, not even ones offering servers in Europe, so the data stays under European jurisdiction
- Hosting in a data centre in Frankfurt, Germany, whose operator is certified for ISO 27001, ISO 27017, ISO 27018 and ISO 27701

3.6 Compliance and service

- Meets EU Directive 2019/1937 and the national laws transposing it
- GDPR compliant, with a data processing agreement in place
- Report data is kept for as long as the organisation instructs and is securely deleted when the service ends
- Automated set-up and implementation, so a channel is live without manual work
- Service levels are set out in the service level agreement