WhistleB

WHISTLEBLOWING CENTRE

WhistleB information security 2020

Quality Control, Certificates, Assessments

WhistleB has made data privacy our top priority. The WhistleB service is continuously monitored and regularly tested, including penetration testing by external IT security experts. Visit the WhistleB Trust Centre » to learn more about whistleblowing and data privacy.

Assessments and Certifications

- ✓ EU GDPR compliance. External assessment according to ISO/IEC 27701:2019.
- ✓ Data Processing Impact Assessment (DPIA), to be used by our customers.
- ✓ ISMS compliance with ISO/IEC 27001:2017. External assessment
- ✓ Regular vulnerability and penetration tests. External assessment
- ✓ Data storage and development (Microsoft Azure): Azure has a multitude of certifications, among these ISO 27001 and ISO 27018 certifications.
- ✓ Cloud Security Alliance, star registry self-assessment.

External assessments

EU General Data Protection Regulation, GDPR, external assessment:

"Altogether the company's WhistleB service is well-engineered from a GDPR perspective. Apart from its fundamental design, which conforms to the most stringent requirements, the service also provides a host of GDPR compliant functions, such as the ability to perform selective purging. These are to be considered very advanced features that are utmost well aligned with GDPR requirements. "

Göran Gräslund, Legal Counsel and former Director General at the Swedish Data Inspection Authority, January 2020

External assessment of Information security management system:

"Security level for data protection of PII (Personally identifiable Information) is corresponding to industry practice and stakeholder expectations and requirements." The concepts "privacy by design" and "privacy by default" are enforced from policy level via development and deployment to operations and compliance activities. Technical solutions including the WhistleB application are designed and maintained on industry and good IT-security practices. Enhanced IT-security competence for application management will be procured and maintained."

Fredrik Rehnström, Fredrik Rehnström Senior security advisor, executive Vice President ROTE Consulting, CISSP, CISM, CISA, CGEIT, CPP, January 2020

Vulnerability and penetration test findings:

"At the time of assessment, the privacy of the whistleblowers is preserved. Outpost24 attacked the application from the Internet and was not able to retrieve sensitive data."

Data security expert Outpost24, vulnerability and penetration test, March 2020.

WhistleB Business ethics in brief

WhistleB has many years of experience in business ethics and sustainability issues. WhistleB offers services related to the establishment and anchoring of code of conducts, ethical policies and sustainability reporting.

- ✓ WhistleB reports sustainability work according to Global Reporting Initiative (GRI). WhistleB GRI Report
- ✓ All employees and subcontractors sign WhistleB Code of Conduct/Supplier Code.
- ✓ WhistleB compensates for the carbon dioxide emissions caused by the business, key source being business travels.
- ✓ WhistleB is a signatory of UN Global Compact https://www.unglobalcompact.org/what-is-gc/participants/134882-WhistleB-Whistleblowing-Centre
- ✓ WhistleB's founders, Gunilla Hadders and Karin Henriksson, are the authors of a Sustainability Handbook; "Sustainable Profit", translated into multiple languages and used by companies and organisations, including the Swedish Ministry for Foreign Affairs.

Technical information, examples of key solutions

The whistleblowing service enables employees and other stakeholders to send a message about their concern, anonymously or openly. Appointed individuals get a notification and log into the Case management tool to read the message and take action.

Encryption

Data is only accessible via the Case management tool, where access is granted to authorised users. The WhistleB System uses a combination of both symmetric and asymmetric cryptographic systems to encrypt all whistleblowing reports, follow-up questions and translations. This encryption method is safe and ensures that only the intended recipient can access the data.

WhistleB handles encrypted data and cannot decrypt the reports to and from a whistleblower. The customer controls the encryption key and is the only party that can decrypt and access the data. No data is stored on mobile devices. In addition, customer data is encrypted on file-level with Transparent Data Encryption (TDE).

Access

The application supports an embedded strong authentication based on .NET authentication schema.

- WhistleB administrators: each user accesses the service with e-mail address and a personal login password (defined by the user) plus two-factor authentication.
- Customer access: Each user accesses the service with e-mail address and a personal login password (defined by the user). Two-factor authentication is added and enforced at the choice of the customer. A so-called secondary password is used to decrypt and access the cases.
- Strong passwords are enforced by the WhistleB system.

Logging

- The communication channel (whistleblower): Data related to whistleblowers is not tracked in order to ensure the whistleblower's anonymity.
- Case Management tool: The customer can follow up case management via the internal case log, i e activities made by the Case or Security manager in the case management tool:
- WhistleB Administrators: All logins are logged. WhistleB administrators do not have access to customer data.

Secure hosting

The WhistleB service platform is designed for high scalability and flexibility, offering a future proof service to our customers. WhistleB have chosen Microsoft Azure as hosting and development platform, offering the most comprehensive set of compliance offerings of any other cloud service provider.

The Azure platform services used by WhistleB are delivered through data centers designed to run 24/7/365, and each employing various measures to protect operations from power failure, physical intrusion, and network outages. Customer data is kept secure through encrypted communications as well as threat management and mitigation practices, including regular penetration testing.

Data is stored within EU/EES: Primary location in Ireland with failover (secondary location) in the Netherlands.

Microsoft Azure are committed to annual ISO/IEC 27001 (international standard for information security management) and ISO/IEC 27018 (international standard for protecting personal data in the cloud) certification. Management Security and compliance statements for Microsoft Azure can be accessed at Microsoft Trust Center portal.