Compliance statement GDPR, 2020

2020-01-31

WhistleB service, Whistleblowing Centre AB

Rote Consulting is an independent audit and advisory company specialized in enterprise risk, security, privacy and continuity management. Rote is also a proud standard developer and active member of the technical committee at SIS for the ISO/IEC 27000 standards since 2003.

Executive summary

The service, WhistleB, is an in-house development by Whistleblowing Centre AB conforming to the most stringent security and privacy by design requirements as expressed in standards and by law such as the European Union General Data Protection Regulation (GDPR). Added to the fundamental privacy and data protection measures embedded in the design are also state of the art features addressing GDPR compliant functions such as selective purging to meet data retention requirements and rights for individuals to have their data blocked or erased when so required. These features provide data controllers with swift functions for granular management of the data and for meeting the rights granted individuals by the regulation.

- Whistleblowing Center AB maintains its information security management system (ISMS) according to SS-EN ISO/IEC 27001:2017
- WhistleB service is assessed for GDPR compliance according to ISO/IEC 27701:2019, the extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines
- Regarding GDPR, the WhistleB service is assessed for compliance in relation to the data processor responsibilities as laid out in ISO/IEC 27701:2019 for the areas;
    - Conditions for collection and processing personal data
        - General statements on information security and privacy compliance
        - Processing purpose legitimacy and specification
        - Data subjects' consent to processing and choice
    - Obligations to personal data principals
        - Openness, transparency and notice
        - Data subjects' rights
        - Use, retention and disclosure limitation
    - Privacy by design and privacy by default
        - Access controls, segregation of duties
        - Data minimization principles
        - Accountability and incident management
    - Personal data sharing, transfer and disclosure
        - Legal purposes in Data Processing Agreements (DPAs)

Security safeguards are meet according to Information Security Policy and non-access to customer Personal Identifiable Information (PII). Supplemental security safeguards may apply for additional, by client defined, data.

Stockholm, January 31, 2020

Göran Gräslund
Legal Counsel and former Director Gen.
Swedish Data Inspection Authority

Mikael Forsström
BA and Senior Consultant
Information Security and Privacy

Table of contents

1 Scope of statement.....1
2 Criteria's for assessment and statement 1
3 Summary.....1
4 Detailed statement.....2
5 Information sources consulted for evaluation.....4

1 Scope of statement

Scope of assignment is to objectively assess and compare Whistleblowing Centre AB's service WhistleB current privacy information security level, with industry practices, Swedish and international standards and relevant stakeholder expectations and requirements.

2 Criteria's for assessment and statement

This statement is based on the assessment of the GDPR privacy information section of Whistleblowing Centre AB's information security management system. The assessment controls have been derived from:

- EU 2016/679 General Data Protection Regulation (GDPR)
- SS EN ISO/IEC 27001:2017 Information Security Management System requirements (corresponds to ISO/IEC 27001:2013 with Cor 1:2014 and Cor 2:2015)
- ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

3 Summary

The security framework within Whistleblowing Center AB is aligned to Swedish and international information security standard according to ISMS Compliance Statement, 2020 (based on assessment according to SS-EN ISO/IEC 27001:2017). This serves as a relevant foundation for the company's technical and operational GDPR compliance.

This evaluation is limited to PII compliance according to GDPR and ISO 27701 code-of-conduct requirements on the company acting as data processor for the service WhistleB.

A key finding in the WhistleB service assessment is that the hosting company Whistleblowing Centre AB does not have access to end-user PII at all, except for corresponding data exposed in the optional professional transaction service. When additional security safeguards are required for GDPR compliance, these have been adequately resolved as follows:

- *Consent and choice* – WhistleB provide system functionality for right to access, correct and erase PII according to customer obligations.
- *Purpose legitimacy and specification* – Records of processing activities are provided by agreed system functionality. It is the customer's responsibility to keep a repository for registered PII.
- *Data minimization* – Temporary files are kept and deleted upon customers instructions.
- *Use, retention and disclosure limitation* – The service does however include logging of every change and access event. This information is provided to customers.
- *Openness, transparency and notice* – WhistleB applies full transparency to customers regarding sub-contractor engagements. This is confirmed in WhistleB security policy and customer agreements.
- *Accountability* – WhistleB PII breach notification are defined according to security policy. The security policy is communicated with customers and compliant to service agreements.
- *Information security* – According to WhistleB security requirements on service are compliant regarding confidentiality obligation, restoration of PII, individual login IDs, User records, reuse of user IDs, contracts with customers, contracts with sub-contractors that process PII, re-assignment of PII storage space.
- *Privacy compliance* – WhistleB storage and transmission is limited according to agreed contracts with customers. However, WhistleB take no responsibility for customer's geographical transmission of information. This is upon the user's responsibility according to customers' instructions. Logging of information access is provided to customers.
- *Privacy by design and default* – Privacy and security measures are considered in the planning phases of software development. Privacy settings, such as access limitation, are applied by default.

Supplemental security safeguards are applied for sub-supplier provided professional translation service.

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 highly advanced features well aligned with GDPR requirements.

4 Detailed statement

GDPR/PII governance assessment, Whistleblowing Center AB

Due to the nature of WhistleB's product line, its entire business culture and organization observes a notably high level of data privacy awareness. All internal process,

communications, and staff meet or exceed requirements for confidentiality and observance of data privacy in accordance with the GDPR. In addition, WhistleB maintains its operations according to ISO/IEC 27701:2019 and observes the necessary requirements in all its processes. This quality culture serves as a sound foundation for its technical and operational GDPR compliance.

According to issued ISMS compliance statement 2020 Whistleblowing Center AB shows that WhistleB information security framework is aligned to Swedish and international information security standards. PII security safeguards analysis are based on the ISMS statements that:

- Technical solutions including the WhistleB application are designed and maintained on industry and good IT-security practices
- Underlying platforms and infrastructure for hosting the WhistleB application are well audited and tested by supplier (MS Azure) and third-party assessors

GDPR/PII service assessment, WhistleB
Assessed PIMS controls in ISO 27701:2019 Information technology - Security techniques - Code of practice for personally identifiable information protection.
Assessed PIMS and GDPR controls as a Processor for WhistleB service.

GDPR/PIMS requirement	Statement	Comments/Improvements
Processing purpose legitimacy and specification	Adequate	WhistleB does not have access to customer PII contacts and content are not used for any other purpose than agreed with customers. Records of processing activities are provided by agreed system functionality. It is the customer's responsibility to keep a repository for registered PII.
Data subjects' consent to processing and choice	Adequate	WhistleB provides system functionality for right to access, correct and erase PII according to customer obligations and the customers have provided WhistleB with information on agreement and legal ground for processing with data subjects, Customer's Privacy Notice.
Openness, transparency and notice	Adequate	WhistleB applies full transparency to customers regarding sub-contractor engagements. This is confirmed in WhistleB security policy and customer agreements.
Data subjects' rights	Adequate	Enhanced features available in the WhistleB service supports activities to respond to data subjects' rights
Use, retention and disclosure limitation	Adequate	WhistleB does not have access to customer PII other than specifically customer selected content provided to sub-supplier for professional translation. No other disclosure of information to third parties is applied. The service does however include logging of every change and access event. This information is provided to customers.
Access controls, segregation of duties	Adequate	The WhistleB service limit accesses to data according to the "need to know" principle

GDPR/PIMS requirement	Statement	Comments/Improvements
Data minimization principles	Adequate	Temporary files are kept and deleted upon customers instructions.
Accountability and incident management	Adequate	WhistleB PII breach notification are defined according to security policy. The security policy is communicated with customers and compliant to service agreements.
Legal purposes in Data Processing Agreements (DPAs)	Adequate	The WhistleB standardized DPA addresses the full set of aspects of Controller-processor relationship as laid out in the GDPR
Information security	Adequate	According to WhistleB security requirements on service are compliant regarding: • Confidentiality obligation • Restoration of PII • Individual login IDs • User records • Reuse of user IDs • Contracts with customers • Contracts with sub-contractors that process PII • Re-assignment of PII storage space Whereas following security safeguards are out of scope as WhistleB have no access* to customer PII, hence the customers' responsibility: • Destruction of hardcopy material • Transfer of media containing PII • Un-encrypted media • Transmission over a public network • Destruction of hardcopy materials *except for specifically customer selected content available for professional translation service where supplemental security safeguards are applied for GDPR compliance.
Privacy compliance	Adequate	WhistleB storage and transmission is limited according to agreed contracts with customers. However, WhistleB take no responsibility for customer's geographical transmission of information. This is upon the user's responsibility according to customers' instructions. Logging of information access is provided to customers.

5 Information sources consulted for evaluation

- Compliance Statement ISMS, WhistleB 2020-01-31
- WhistleB DPIA 2019
- Additional Questionnaire for ISO 27701 processor assessment