

Privacy policy for the whistleblower system of secunet Security Networks AG

Notes on data protection

In the following, we would like to inform you about the collection, processing and use of personal data within the framework of the secunet Security Networks AG whistleblower system in accordance with Art. 13 and 14 GDPR. Your personal data is collected, processed and used as soon as you submit a report by e-mail, telephone call, letter, personal appearance in the Compliance Office or via the EQS Integrity Line whistleblower system of EQS Group. The legal requirements for the processing of personal data are set out in the GDPR and the German Federal Data Protection Act (BDSG). Please read this data protection information carefully before submitting a report.

Responsible person/ your contact person

Your contact within the meaning of the GDPR and other data protection laws applicable in the member states of the European Union (EU) is

secunet Security Networks AG
Kurfürstenstrasse 58
45138 Essen

Executive Board: Marc-Julian Siewert (Chairman of the Executive Board), Torsten Henn, Dr Kai Martius, Jessica Nospers
Phone: +49 (0) 201 5454-0
Fax: +49 (0) 201 5454-1000
E-Mail: info@secunet.com

You can contact our data protection officer at the above address or at datenschutz@secunet.com

Processed data

The whistleblower system is used on a voluntary basis. If you submit a report or complaint via the whistleblower system, we collect the following personal data and information:

- Your name and contact details (business and/or private), if you disclose your identity,
- the fact that you have made a report and in what form,
- Further data on the notification (e.g. time, content and other circumstances of the notification),
- Information on relevant facts including any attachments you may have provided and any privately described content,
- whether you are employed by secunet,
- if applicable, names of persons and other personal data of the persons you name in your notification,
- if applicable, special categories of personal data, provided that your information contains corresponding data and the clarification measures make it necessary to process the data in accordance with the law.

Privacy policy for the whistleblower system of secunet Security Networks AG		Page1 from 4
Validity from:	February 2025	
Version no:	1.2 from 10/07/2025	

Reason and purpose of data processing

secunet Security Networks AG must ensure compliance with the applicable statutory provisions within the scope of its business operations. This applies to the provisions of criminal law, the German Administrative Offences Act, tax law, data protection law, stock corporation law, labour law, antitrust law, the German Supply Chain Duties Act (LkSG) and other binding legal requirements. In the event of a breach of the aforementioned legal provisions, secunet Security Networks AG may be subject to fines or imprisonment, penalties, claims for damages or reputational damage. To counteract this, secunet Group has taken appropriate measures to ensure compliance with legal regulations and internal rules within the company. One of these measures is the whistleblower system/complaints procedure.

The purpose of the whistleblower system is to receive and process reports of violations of the law or internal regulations against secunet Security Networks AG in a secure and confidential manner. The purpose of data processing as part of the complaints procedure is to accept and clarify serious suspected cases of violations of human rights and environmental due diligence obligations.

secunet Security Networks AG processes your data within the framework of the applicable laws, in particular for the following specific compliance and information purposes:

- plausibility check
- if necessary, communication with the whistleblower or complainant, e.g. for further questions about the reported facts
- investigation of misconduct, e.g. fraud, corruption offences, antitrust violations and other violations of the secunet Code of Conduct
- clarification of serious suspected cases of violations of human rights and environmental due diligence obligations
- implementation of legal obligations e.g. §§30, 130 OWiG, §§ 93, 111 AktG
- prevention of future misconduct
- legal proceedings
- examination of relevance for the subsidiaries
- implementation of the duty to cooperate
- documentation of whistleblower and complaints procedures

If the Compliance Office intends to further process the personal data for a purpose other than that for which the personal data was collected, it shall provide the data subject with information on this other purpose and all other relevant information in accordance with Art. 13 para. 2 GDPR prior to disclosure.

Legal basis for the processing of data

secunet Security Networks AG may base authorised data processing in the context of reconnaissance measures in particular on the following legal bases:

The processing of personal data within the framework of the whistleblower system is carried out on the basis of the **legal provisions** applicable to secunet (Art. 6 para. 1 lit. c GDPR), in particular §8 of the LkSG and Directive 2019/1937 of the EU or the German Whistleblower Protection Act. The processing of personal data within the framework of the whistleblower system is based on secunet's legitimate interests in the detection and prevention of

Privacy policy for the whistleblower system of secunet Security Networks AG		Page2 from 4
Validity from:	February 2025	
Version no:	1.2 from 10/07/2025	

wrongdoing and the associated avoidance of damage and liability risks for secunet Security Networks AG (Art. 6 para. 1 lit. f GDPR) in conjunction with Sections 30, 130 of the German Administrative Offences Act. §§ Sections 30, 130 of the German Administrative Offences Act (OWiG) and Sections 93, 111 of the German Stock Corporation Act (AktG).

If a report or complaint received concerns an employee of secunet Security Networks AG, the processing also serves to prevent criminal offences and other legal violations in connection with the **employment relationship** (Section 26 (1) BDSG).

Personal data of the whistleblower will only be processed with their **consent** (Art. 6 para. 1 lit. a GDPR), which is given by the fact that the report can also be submitted anonymously.

Recipients of the personal data

If you submit a report via the secunet Security Networks AG whistleblower system, your data will be forwarded directly to the Compliance Office for the purpose of processing and checking the report.

The Compliance Office examines the reported facts and, if necessary, carries out further clarification of the facts; the data is always treated confidentially. If false information is knowingly provided with the aim of discrediting a person, the confidentiality of the data is always guaranteed; if necessary, it will be disclosed to the responsible authorities/offices.

In certain cases, secunet Security Networks AG is legally obliged to inform the accused person of the allegations made against them. This is required by law if it is objectively established that the provision of information to the accused can no longer affect the concrete clarification of the information.

As far as legally possible, your identity as a whistleblower will not be disclosed and it will also be ensured that no conclusions can be drawn about your identity (Art. 14 para. 3 lit. a GDPR).

If necessary to clarify the facts of the case, personal data may be transmitted to individual selected persons of secunet Security Networks AG or – if also affected by the facts of the case – to subsidiaries of secunet to the extent necessary. Every person who receives access to the personal data is obliged to maintain confidentiality. If required by law or in justified cases, data may be transferred to law enforcement authorities, antitrust authorities, other administrative authorities, courts and authorised law firms and auditing companies.

Duration of data storage

secunet Security Networks AG uses technical and organisational measures (TOMs) to protect the personal data to be managed through the use of the whistleblowing system/complaints procedure from unauthorised access, disclosure, misuse, manipulation, loss and destruction during its collection, processing and use. Our security measures are continuously improved and adapted in line with the state of the art.

Personal data will be stored for as long as required for the clarification and final assessment, secunet has a legitimate interest or there is a legal requirement. The duration of storage in individual cases depends in particular on the criticality of the reported breach of duty. Your data will be deleted in accordance with the legal requirements as soon as it is no longer required to achieve the purpose of the data processing, secunet has no legitimate interest in storing it or the legally prescribed storage period has expired.

Privacy policy for the whistleblower system of secunet Security Networks AG		Page3 from 4
Validity from:	February 2025	
Version no:	1.2 from 10/07/2025	

Automated decision-making

No automated decision-making including profiling in accordance with Art. 22 GDPR takes place as part of the whistleblower system.

Third country transfers

The personal data is processed within the EEA and the EU. If the Compliance Office intends to transfer the personal data to third countries, e.g. to clarify the facts of the case or due to a legal obligation, this intention will be communicated to the data subject at the time of collection. The EQS Integrity Line server is located in a high-security data centre in the European Union, so that a transfer of the data to a third country can be ruled out.

Your rights as a data subject

As part of the processing of your personal data, you also have certain rights under the EU GDPR:

- the right to information in accordance with Art. 15 GDPR – whether and which of your data is processed,
- the right to rectification in accordance with Art. 16 GDPR of incorrect or incomplete data,
- the right to erasure of data under the conditions specified in Art. 17 GDPR,
- the right to restrict processing to certain purposes under the conditions of Art. 18 GDPR,
- the right to data portability under the conditions set out in Art. 20 GDPR,
- the right to withdraw your consent at any time. Your revocation does not affect the legality of the processing of the data processed up to that point on the basis of your consent,
- the right to object to certain data agreements referred to in Art. 21 GDPR,
- the right to lodge a complaint with a supervisory authority in accordance with Art. 77 GDPR if you believe that the processing of your data violates the GDPR.

You can send this objection informally by e-mail or by post to the contact details listed under "Responsible person/your contact person".

Changes to the privacy policy

We reserve the right to amend the privacy policy in order to adapt it to changed legal situations or in the event of changes to the services and data processing.

secunet Security Networks AG

Privacy policy for the whistleblower system of secunet Security Networks AG		Page4 from 4
Validity from:	February 2025	
Version no:	1.2 from 10/07/2025	