

Privacy Notice for the Whistleblowing System of secunet Security Networks AG

Data protection information

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

Controller / your contact

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, Germany

Executive Board: Marc-Julian Siewert (Chairman), Torsten Henn, Dr. Kai Martius

Phone: +49 (0) 201 5454-0
Fax: +49 (0) 201 5454-1000
Email: info@secunet.com

You can reach our Data Protection Officer at the above address or at datenschutz@secunet.com

Data processed

Use of the whistleblowing system is voluntary. If you submit a report or complaint via the whistleblowing 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 submitted a report and in what form,
- further data relating to the report (e.g. time, content and other circumstances of the report),
- information on relevant facts, including any attachments you provide and any private matters you describe,
- whether you are employed by secunet,
- where applicable, names of persons and other personal data of the persons you name in your report,
- where applicable, special categories of personal data, if your report contains such data and the investigative measures require the lawful processing of that data.

Privacy Notice for the Whistleblowing System of secunet Security Networks AG		Page 1 of 4
Valid from:	February 2025	
Version no.:	1.3 of 5 October 2026	

Reason for and purpose of data processing

secunet Security Networks AG must ensure compliance with applicable laws in the course of its business operations. This applies to the requirements of criminal law, the Administrative Offences Act, tax law, data protection law, stock corporation law, labour law, competition law, the Supply Chain Due Diligence Act (LkSG) and other binding legal requirements. Violations of these laws may expose secunet Security Networks AG to fines or imprisonment, administrative penalties, claims for damages or reputational harm. To counter these risks, the secunet Group has taken appropriate measures to ensure compliance with legal requirements and internal rules within the company. One of these measures is the whistleblowing system / complaints procedure.

The whistleblowing system serves to receive and handle reports of violations of laws or internal rules against secunet Security Networks AG in a secure and confidential manner. The purpose of data processing within the complaints procedure is to receive and investigate serious suspected violations of human rights and environmental due diligence obligations.

Within the scope of applicable law, secunet Security Networks AG processes your data in particular for the following specific compliance and investigative purposes:

- plausibility check
- where necessary, communication with the whistleblower or complainant, e.g. in the event of further questions about the reported matter
- investigation of misconduct, e.g. fraud, corruption offences, competition law violations and other breaches of the secunet codes of conduct
- investigation of serious suspected violations of human rights and environmental due diligence obligations
- fulfilment of legal obligations, e.g. Sections 30 and 130 of the Administrative Offences Act (OWiG), Sections 93 and 111 of the Stock Corporation Act (AktG)
- prevention of future misconduct
- court proceedings
- assessment of relevance for subsidiaries
- fulfilment of duties to cooperate
- documentation of whistleblowing and complaints procedures

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

Legal bases for data processing

In the context of investigative measures, secunet Security Networks AG may base permissible data processing in particular on the following legal bases:

Personal data is processed within the whistleblowing system on the basis of the **statutory provisions** applicable to secunet (Art. 6(1)(c) GDPR), in particular Section 8 LkSG and Directive (EU) 2019/1937 and the German Whistleblower Protection Act (HinSchG). Personal data is also processed within the whistleblowing system on the basis of secunet's legitimate interests in detecting and preventing misconduct and thereby averting damage and liability risks for secunet Security Networks AG (Art. 6(1)(f) GDPR) in conjunction with Sections 30 and 130 of the Administrative Offences Act (OWiG) and Sections 93 and 111 of the Stock Corporation Act (AktG).

Privacy Notice for the Whistleblowing System of secunet Security Networks AG		Page 2 of 4
Valid from:	February 2025	
Version no.:	1.3 of 5 October 2026	

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

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

Recipients of personal data

If you submit a report via the whistleblowing system of secunet Security Networks AG, your data is forwarded directly to the Compliance Office for the purpose of processing and reviewing the report.

The Compliance Office reviews the reported matter and, where necessary, conducts a further investigation; the data is always treated confidentially. If false reports are knowingly submitted with the aim of discrediting a person, the confidentiality of the data cannot be guaranteed, and the data may be disclosed to the competent authorities or bodies.

In certain cases, secunet Security Networks AG is legally obliged to inform the accused person of the allegations made against them. This is legally required once it is objectively established that informing the accused person can no longer impair the investigation of the specific report.

In doing so, your identity as a whistleblower will not be disclosed, to the extent legally possible, and it will additionally be ensured that no conclusions can be drawn about your identity (Art. 14(3)(a) GDPR).

Where necessary to investigate the matter, personal data may be transferred to selected individuals within secunet Security Networks AG or, if they are also affected by the matter, to secunet subsidiaries to the extent required. Every person who is given access to the personal data is bound to confidentiality. Where legally required or in justified cases, data may be transferred to law enforcement authorities, competition authorities, other administrative authorities, courts, and engaged law firms and audit firms.

Duration of data storage

secunet Security Networks AG uses technical and organisational measures (TOMs) to protect the personal data managed through the whistleblowing system / complaints procedure against 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 is retained for as long as required for the investigation and final assessment, or as long as secunet has a legitimate interest or a legal requirement exists. The storage period depends in each individual case in particular on the criticality of the reported violation. Your data will be deleted in accordance with the statutory requirements as soon as it is no longer necessary to achieve the purpose of the processing, secunet no longer has a legitimate interest in storing it, or the statutory retention period has expired.

Automated decision-making

No automated decision-making, including profiling, within the meaning of Art. 22 GDPR takes place within the whistleblowing system.

Privacy Notice for the Whistleblowing System of secunet Security Networks AG		Page 3 of 4
Valid from:	February 2025	
Version no.:	1.3 of 5 October 2026	

Transfers to third countries

Personal data is processed within the EEA and the EU. Should the Compliance Office intend to transfer personal data to third countries, e.g. to investigate the matter or due to a legal obligation, the data subject will be informed of this intention 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 data to a third country can be ruled out.

Your rights as a data subject

With regard to the processing of your personal data, you also have certain rights under the EU GDPR:

- the right of access under Art. 15 GDPR – whether and which of your data is being processed,
- the right to rectification of inaccurate or incomplete data under Art. 16 GDPR,
- the right to erasure of data under the conditions set out in detail in Art. 17 GDPR,
- the right to restriction of 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 consent at any time. Withdrawal does not affect the lawfulness of processing carried out on the basis of your consent before its withdrawal,
- the right to object to certain data processing operations specified in Art. 21 GDPR,
- the right to lodge a complaint with a supervisory authority under Art. 77 GDPR if you believe that the processing of your data violates the GDPR.

You may send such an objection informally by email or post to the contact details listed under “Controller / your contact”.

Changes to this privacy notice

We reserve the right to amend this privacy notice in order to adapt it to changes in the legal situation or to changes in our services and data processing.

secunet Security Networks AG

Privacy Notice for the Whistleblowing System of secunet Security Networks AG		Page 4 of 4
Valid from:	February 2025	
Version no.:	1.3 of 5 October 2026	