Data Protection Statement for the Whistleblowing System of secunet Security Networks AG

Data protection policy

In the following section, we would like to inform you about how personal data is collected, processed and used as part of the secunet Security Networks AG whistleblowing 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 email, telephone call, letter, or in person at the Compliance Office or via the BKMS Whistleblowing System. The legal requirements governing 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.

Controller / your contact person

Your contact person as defined by 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

Management Board: Axel Deininger (CEO), Torsten Henn, Dr Kai Martius, Thomas Pleines
Tel: +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

Use of the whistleblowing system is voluntary. When 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 made a report and the form thereof,
- further details of the report (e.g. time, content and other aspects of the report),
- information on relevant facts, including any attachments you may have provided and any privately disclosed content,
- whether you are employed by secunet,
- if applicable, names of people and other personal details of the people you name in your report,
- if applicable, special categories of personal data, provided that your report contains such data and the clarification measures make it necessary to process the data in accordance with the law.

Reason for and purpose of data processing

secunet Security Networks AG must ensure compliance with the applicable statutory provisions 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, antitrust law, the Supply Chain Due Diligence Act (LkSG) and other binding legal requirements. In the event of a breach of the aforementioned statutory provisions, secunet Security Networks AG may be subject to fines or imprisonment, claims for damages or reputational damage. To counteract this, secunet Group has taken appropriate measures to ensure compliance with legal requirements and internal regulations within the company. One of these measures is the whistleblowing system / complaints procedure.

The purpose of the whistleblowing system is to collect and process information about breaches of the law or internal regulations relating to secunet Security Networks AG in a secure and confidential manner. The purpose of data processing as part of the complaints procedure is to receive and clarify serious suspected cases of human rights and environmental due diligence breaches.

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

- Plausibility check
- If necessary, communication with the whistleblower or complainant, for example if there are further queries regarding the reported facts
- Investigation of misconduct, e.g. fraud, corruption offences, antitrust breaches

and other breaches of the secunet Code of Conduct

- Clarification of serious suspected cases of breaches of human rights and environmental due diligence obligations
- Implementation of legal obligations e.g. Sections 30, 130 German Administrative Offences Act (OWiG), Sections 93, 111 German Stock Corporation Act (AktG)
- Prevention of future misconduct
- Legal proceedings
- Examination of relevance for the subsidiaries
- Implementation of duties to cooperate
- Documentation of whistleblower and complaints procedures

If the Compliance Office intends to process the personal data for a purpose that is different to that for which the personal data was collected, it shall provide the data subject with information about 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 its authorised data processing activities relating to clarification measures on the following legal bases in particular:

The processing of personal data in the context of the whistleblowing system is based on the **legal provisions** applicable to secunet (Art. 6 para. 1 lit. c GDPR), in particular Section 8 of LkSG and Directive 2019/1937 of the EU or the Whistleblower Protection Act. The processing of personal data in the context of the whistleblowing system is based on secunet's legitimate interests in the identification and prevention of malpractice 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 (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 activity also serves to prevent criminal offences and other legal breaches in connection with the **employment relationship** (Section 26 (1) BDSG).

The personal data of the whistleblower will only be processed with their **consent** (Art. 6 para. 1 lit. a GDPR), which is ensured 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 whistleblowing system, your data will be forwarded directly to the Compliance Office for the purpose of processing and reviewing the report.

The Compliance Office examines the reported matter and, if necessary, clarifies the facts in greater detail; 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/bodies.

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 providing information to the accused can no longer impair the actual investigation.

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

If deemed necessary to clarify the facts of the case, personal data may be transmitted to individual selected persons of secunet Security Networks AG or – if they are also affected by the facts of the case – to subsidiaries of secunet to the extent necessary. Every person who has access to personal data is obliged to treat it confidentially. If required by law or in justified cases, data may be transmitted 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 that is managed

through the use of the whistleblowing system / complaints procedure from unauthorised access, disclosure, misuse, manipulation, loss and destruction when it is collected, processed and used. Our security measures are continuously improved and adapted according to the state of the art.

Personal data will be stored for as long as required for clarification and final judgement, or if a legitimate interest of secunet or a legal requirement exists. In certain cases, the duration of storage will depend in particular on the criticality of the reported breach of duty. Your data will be erased in accordance with the statutory provisions as soon as it is no longer required for fulfilling the purpose of data processing, secunet has no legitimate interest in storing it or the statutory retention period has expired.

Automated decision making

The whistleblowing system does not involve automated decision-making or profiling as defined in Art. 22 GDPR.

Transfer to third countries

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 BKMS server is located in a high-security data centre in Germany, meaning that the transfer of data to a third country can be ruled out.

Your rights as a data subject

You also have certain rights in relation to the processing of your personal data under the EU GDPR:

- the right to information pursuant to Art. 15 GDPR - whether your data is being processed and, if so, which data,
- the right to rectification pursuant to Art. 16 GDPR of inaccurate or incomplete data,
- the right to erasure of data under the conditions specified in Art. 17 GDPR,
- the right to restrict processing to specific 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. Your withdrawal of consent does not affect the legitimacy of the data processing carried out on the basis of your consent up to that point,
- the right to object to certain data agreements referred to in Art. 21 GDPR,
- the right to lodge a complaint with a supervisory authority pursuant to Art. 77 GDPR if you believe that the processing of your data is in breach of GDPR.

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

Changes to the data protection statement

We reserve the right to change the data protection statement in order to adapt it to changed legal situations or in the event of changes to the services and to the data processing.

secunet Security Networks AG