

Ethics and Compliance Helpline Data Protection and Privacy Notice

1. Purpose

The data privacy regulations of some countries require that a person making a report containing personal data must be notified of certain collection and retention practices regarding the information submitted by that person through this service.

If you do not wish to accept the terms below, we may be unable to accept any information through this system and suggest you report this matter directly to your supervisor or manager or to a member of the Ethics and Compliance or People Success organizations, depending on the nature of the possible violation.

2. General

This service is a web and phone-based intake system provided by McAfee to its employees, vendors, suppliers and business partners and those of its subsidiaries (“Reporters”) for reporting suspected violations of laws or regulations or suspected violations of company policies. Depending on the jurisdiction, suspected violations of company policies might not fall into material scope of a specific whistleblower regulation.

McAfee is the controller of the processing, and NAVEX is a processor acting on behalf of McAfee. You may contact McAfee with any questions relating to this Notice or this service at protectprivacy@mcafee.com. If you are a resident of the European Union or the United Kingdom and you have any questions about this Notice or this service, you may also contact the McAfee Data Protection Officer at:

Attn: McAfee Data Protection Officer
Data Business Services
Nördliche Münchner Straße 47
D-82031 Grünwald/ München
Germany
+49 (0)89 12501375-0

3. Use of this service

Use of this service is entirely voluntary. The service is a confidential online reporting system that allows you to report suspected violations of the law or company policies, as well as other concerns you may have, to McAfee.

Please be aware that the information you supply about yourself, your colleagues, or any aspect of the company's operations may result in decisions that affect others. Therefore, we ask that you only provide information that you believe is true. You will not be subject to retaliation from McAfee for any report of a suspected violation that is made in good faith, even if it later turns out to be factually incorrect.

Please be aware, however, that knowingly providing false or misleading information will not be tolerated. The information you submit will be treated confidentially except in cases where this is not possible because of legal requirements or in order to conduct an investigation, in which case the information will be handled sensitively. We encourage you to identify yourself in order for us to follow up with questions we may have.

4. What personal data and information is collected and processed?

This service captures the following personal data and information that you provide when you make a report: (i) your name and contact details (unless you report anonymously) and whether you are employed by McAfee; (ii) the name and other personal data of the persons you name in your report if you provide such information (i.e.: description of functions and contact details); and (iii) a description of the alleged misconduct as well as a description of the circumstances of the incident. Note that depending upon the laws of the country in which you are residing, the report may not be made anonymously; however, your personal information will be treated confidentially and will only be disclosed as set out below.

5. How will the personal data and information be processed after your report and who may access personal data and information?

The purpose for which your personal data, and your report, will be to investigate the issues raised in your report, and to take appropriate follow-up action in accordance with applicable law.

The personal data and information you provide will be stored in a database which is located on servers hosted and operated by NAVEX. NAVEX has entered into contractual commitments with McAfee to secure the information you provide in accordance with applicable law. NAVEX is committed to maintaining stringent privacy and security practices including those related to notice, choice, onward transfer, security, data integrity, access, and enforcement. You may contact McAfee with any requests relating to the use, transfer, correction, or deletion of any of your personal data stored by this service.

For the purpose of processing and investigating your report and subject to the provisions of local law, the personal data and information you provide may be accessed, processed and used by the relevant personnel of McAfee, including Ethics and Compliance, People Success, Internal Audit, Legal, , management, external advisors (e.g. legal advisors), or, in limited circumstances, by technical staff at NAVEX. Those individuals may be located in the United States, the United Kingdom or elsewhere.

Personal data and information you provide may also be disclosed to law enforcement or regulatory authorities. The relevant bodies that receive and process personal data can be located in the US or in another country that may not provide the level of data protection available in the EU.

6. Retention of the report and your data

Your report and your personal data will only be retained for as long as they are needed for the investigation of your allegations, for any legitimate follow-up to the investigation, or as otherwise consistent with law; they will be fully and securely destroyed or erased when and as soon as they are no longer needed for the

investigation of the report, or for the purposes of legitimate follow-up to the report (including legal action). However, reports and files on the investigation of reports (or parts of such reports or files) and personal data in such reports or files may be placed in an archive if there is a clear and overriding public interest or legal interest of McAfee in retaining the data, subject to such restrictions on access to the data aimed at safeguarding the rights and freedoms of the data subjects as may be allowed by applicable law.

7. Your rights

You may exercise rights you may have as a data subject under applicable law, i.e., your:

- right of access to your data;
- right to rectification of incorrect data;
- right to erasure of data (“right to be forgotten”);
- right to ask for restriction (“blocking”) of contested data;
- right to have third parties who received incorrect, incomplete or contested data informed of any rectifications or blocking of your data;
- right to data portability;
- right to object to processing;
- right not to be subject to automated decision-making including profiling (in fact we will not use your data or any information in your report for such decision-making).

We will only restrict any of the above rights if and to the extent that that is necessary and proportionate in order to safeguard any of the major public interests recognized in applicable law such as the protection of criminal investigations or public security, or to protect the fundamental rights and freedoms of others, including any person(s) incriminated in your report, in accordance with applicable law.

In addition to the rights listed above, you may also have the right to lodge a complaint about our processing of your personal data with the authority competent for supervising the processing of personal data (often referred to as the data

protection authority) in the country where you live (if that is an EU/EEA Member State).

8. Transfers of personal data

Your report and your details may be held on the secure servers hosted by NAVEX; may be transferred to NAVEX sub-processors outside your location for service and support or translation and interpretation purposes; and may be passed on to the servers of McAfee, subject to appropriate safeguards.

9. Special country regulations

Some countries restrict reports such that only employees in key or management functions may be the subject of a report. In some countries, anonymous reports may not be permitted under the law except under extremely restrictive circumstances.

Further, any issues or concerns relating to topics not in scope to be reported via this service for a particular country or jurisdiction should be reported directly to your manager or a representative of the Ethics and Compliance, Legal, or People Success organizations as appropriate.