

KEYSIGHT COMPLIANCE HOTLINE DATA PRIVACY NOTICE

Keysight recognizes that individuals have a right to the protection of their personal data¹ and to clear and transparent information about Keysight's personal data processing activities. This Compliance Hotline Data Privacy Notice provides you with a clear and transparent explanation of Keysight's processing of personal data submitted via the Keysight Compliance Hotline, whether by phone or online.

1. Overview

When you submit a report to Keysight's Compliance Hotline, whether online or through a telephone call, any personal data you provide will be processed for the purposes of Keysight's legitimate interests in investigating and remediating allegations of misconduct. Keysight Technologies' Compliance Hotline is operated by NAVEX Global, a data processor and service provider acting on Keysight's behalf to gather information from anyone who makes a report through this Hotline. NAVEX Global will send a report containing the information you provide to Keysight's Compliance Hotline, including any personal data, to designated members of Keysight's Compliance, Internal Audit and/or Human Resources teams. Keysight will treat your report confidentially and with sensitivity and will use the information and personal data for the purposes of investigating and remediating allegations of misconduct.

2. Anonymous reporting

You may make your report anonymously or you may choose to identify yourself. If you wish to report anonymously, you should not include information that may personally identify you. Keysight encourages you to identify yourself, however, so that we may communicate with you as we investigate and resolve your concern. Keysight strictly prohibits retaliation against anyone who makes a report in good faith. Keysight therefore protects the confidentiality of your identity to the extent allowable by law. If you report concerns about a specific Keysight employee, he or she will not receive a copy of your report. Where required by local regulations, Keysight may be required to inform each person implicated in a report within a certain period of time or at the conclusion of the investigation. To the extent legally permissible, Keysight will not disclose your name or identity to the person or people who are the subject of your report.

3. Collection of personal data

The Compliance Hotline may capture the following types of personal data and information if you provide it when making a report: (i) your name and contact details (unless you report anonymously) and whether you are employed by your organization; (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.

4. Disclosure of personal data

Keysight will not share your personal data with third parties outside of Keysight, other than vendors or service providers (such as attorneys or investigators) acting on Keysight's behalf. Such vendors provide

¹ For the purposes of this policy, "personal data" means any information relating to an identified or identifiable natural person. "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

KEYSIGHT COMPLIANCE HOTLINE DATA PRIVACY NOTICE

services pursuant to contracts requiring safeguards for the protection of your personal data, including SCCs where applicable.

Keysight also may disclose your personal data: (a) if we are required to do so by law; (b) if we believe that it is necessary to enforce or apply our terms of use and other agreements or otherwise protect and defend the rights, property or safety of Keysight or that of our customers; or (c) to comply with a judicial proceeding, bankruptcy proceeding, court order or other legal obligation or government inquiry.

5. International transfers of personal data

Keysight's global organizational structure requires the global transfer of personal data within the Keysight group of companies. As a result, we may transfer personal data to, and store or process personal data in, countries other than the country in which the personal data originally was collected. Keysight has executed data processing agreements between and among Keysight entities operating in different countries that contain Standard Contractual Clauses ("SCCs") as defined in the E.U. Data Protection Directive (95/46/EC) and as further authorized in the E.U. General Data Protection Regulation ("GDPR") Article 46(5), to ensure that adequate safeguards are in place for the protection of personal data.

6. Storage and retention of personal data

Keysight will retain personal data you submit via the Hotline for a period of six years after the investigation into your report is closed, unless otherwise prohibited by law. However, Keysight reserves the right to retain your personal data for a longer period of time as necessary to comply with legal obligations or resolve disputes.

7. Your rights regarding to your personal data

You have certain rights with respect to your personal data, including: the right to information about the personal data we store about you, the right to have your personal data corrected if it is inaccurate, and the right to object, on grounds relating your particular situation, at any time to processing of your personal data. You also have the right, under certain circumstances, to erasure, restriction of processing, and portability of your personal data. To exercise your rights please contact Keysight's [Privacy Advocate](#). We will respond to your request as soon as is reasonably practicable and in any event within 30 days. To protect your privacy and security, we will also take reasonable steps to verify your identity before granting you access or enabling you to make corrections.

If you believe that the collection or processing of your personal data by Keysight is not compliant with applicable data protection laws, or have a privacy or data use concern you may contact Keysight's [Privacy Advocate](#), and you have the right also to contact the data protection authority in your country of residence. In Germany, you may also contact Keysight's German Data Protection Officer, Keysight Technologies Germany GmbH, at data-protection_germany@keysight.com.