

DATA PROTECTION & PRIVACY NOTICE

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 and must accept the terms and conditions for the use of this service.

You are being asked to read and accept the terms contained below. If you do not wish to accept the terms below, we suggest you report this matter through Cordaid's other reporting channels, such as your immediate or higher supervisor, the Integrity Focal Point or Officer, or via the reporting channels of Caritas Internationalis or the ACT Alliance, depending on the nature of the possible violation.

1. General

This service is a web-based intake system provided by your organization to its employees, vendors, suppliers and business partners and those of its subsidiaries, as well as other third parties, for reporting suspected violations of laws or regulations, our Code of Conduct or organizational policies.

In certain countries, this service may also be used to report suspected violations of other matters. This service and the database in which the personal data and information that you may report is stored, are operated by NAVEX Global.

To proceed further, please read this notice in its entirety.

2. Use of this service

Use of this service is entirely voluntary. You can alternatively report possible violations using any of the above-mentioned reporting channels.

The purpose of this service is to provide a confidential online reporting system that allows you to report suspected violations of law or organizational policies, as well as other concerns you may have, to your organization. In certain countries, your organization may only accept reports through this service on limited topics, generally restricted to financial, accounting, auditing, bribery, competition law, discrimination and harassment and environment, health, hygiene, and safety matters. If your concern pertains to a matter that, under local law, may not be accepted by your organization through this service, you will need to use one of the alternative reporting channels mentioned above.

Please be aware that the information you supply about yourself, your colleagues, or any aspect of the organizations' 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 your organization 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 and may constitute misconduct in itself if it is proven that false information was provided deliberately. 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.

3. 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 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. Note that some country laws may not allow anonymous reporting; however, your personal information will be treated confidentially and will only be disclosed as set out below.

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

The personal data and information you provide will be stored in a database which is located on servers hosted and operated by NAVEX Global in Germany. NAVEX Global has entered into contractual commitments with your organization to secure the information you provide in accordance with applicable law. Personal data and information provided in a report may be transferred outside of the United Kingdom, the European Union, and/or the European Economic Area for the purpose of providing interpretations or administration of this service. NAVEX Global is committed to maintaining compliance with applicable data protection requirements and adheres to stringent privacy and security practices. 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 your organization, including Human Resources, Finance, Internal Audit, Legal, Corporate Compliance, management, external advisors (e.g. legal advisors), or, in limited circumstances, by technical staff at NAVEX Global. Those individuals may be located in the United States or elsewhere.

Personal data and information you provide may also be disclosed to the police and/or other enforcement or regulatory authorities. Where in line with applicable privacy regulations, relevant information about misconduct stemming from your report may also be shared with third parties, such as via accumulated case metrics and/or information about an individual's misconduct history. This will be done on a strict need-to-know basis and no identifying information about the reporter will be shared unless required by law. 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 or other jurisdictions with more stringent data protection laws.

The personal data you provide will be kept as long as necessary to process your report, or, if applicable, as long as necessary to initiate sanctions or to meet our legal or financial needs.

5. Accessing information concerning the report

The subject of a report will be notified according to the investigation plan. Notice may be delayed or deferred to ensure the integrity of the investigation, preservation of relevant information, and the safety and well-being of all individuals involved.

Further, you have the right to request access, correction, or erasure of personal data or to object to the processing or receive a copy of the personal data held through this service. Any such request should be directed to your organization. You also have the right to lodge a complaint with the relevant supervisory authority.

In some cases, the subject of the report may access information concerning the report, including the source from which the report originates (with the exception of the identity of the reporter), and request correction of personal data that is inaccurate or incomplete in accordance with applicable law. To make any such corrections, please contact the General Counsel or the Corporate Compliance Officer.

6. Special country regulations

Throughout much of the European Union and surrounding areas, reports can only be made relating to limited topics, typically accounting, auditing, bribery, competition law, discrimination and harassment and environment, health, hygiene, and safety matters. Further, some countries restrict reports such that only employees in key or management functions may be the subject of a report.

Any issues or concerns relating to topics not permitted by law to be reported via this service should be reported directly via the alternative reporting channels mentioned above, as appropriate for the subject matter of the possible violation. In some countries, anonymous reports may not be permitted under the law except under extremely restrictive circumstances.

I CONSENT

I have read and expressly consent to the processing of my personal information as described in above.