Data privacy statement: Zurich Ethics Line

This privacy statement explains the information that is collected by Zurich Insurance Company Ltd and the respective subsidiaries ("we", "our, "us") through the Zurich Ethics Line ("platform") and how this data will be processed.

We take privacy very seriously and our goal is always to be transparent. Please read this privacy statement carefully as it contains important information about how we will use your personal data.

When you submit a question or report through the Zurich Ethics Line, it may be accessible as required by Compliance, HR and Legal at the local, regional, and Group levels to ensure accountability and that the report is handled appropriately. If you do not wish to have the report visible outside of your country, please contact your local Compliance or Legal representative directly and raise the concern with them before submitting a report in this platform.

Only with regard to Zurich Cover More, by submitting your question or report you agree that we will share your question or report, or your personal data (where relevant and unless you report anonymously), with other members of the Group (most likely with a Triage Committee based in NA (US)) on a need-to-know basis.

Last Updated 25 January 2025

Data controller and contact details:

Zurich Insurance Company Ltd, Mythenquai 2, 8002 Zurich, Switzerland, and respective subsidiaries you are interacting with act as joint data controllers with respect to this platform.

For any data protection related comment or question you may have in connection with the platform, you can contact the respective subsidiaries' privacy team or reach us by email at privacy@zurich.com.

Additional local data privacy information, where applicable, can be found here.

What personal data may be collected and processed?

Personal data is any information that relates to an identified or identifiable person.

This platform may capture the following personal data that you provide when you submit/update a report or question:

- your name and contact details (unless you report anonymously) and whether you are employed by the organization;
- the name and other personal data of the persons you name in your submission if you provide such information (i.e., description of functions and contact details); and
- a description of the question or allegation, as well as a description of the circumstances of the incident.

The laws of some countries may not permit reports to be made anonymously; however, your personal data will be treated confidentially and will only be disclosed as set out in this privacy statement.

For what purposes do we process your personal data?

We process your personal data to enable us to receive, investigate, and resolve allegations and questions regarding ethics and compliance in a consistent manner in the group.

On what legal basis do we process your personal data?

We process your personal data based on legitimate interest, in order to monitor compliance with laws, regulations, internal policies and our Code of Conduct in a consistent manner in the group.

In countries where whistleblowing systems are required by regulation, the legal basis is to comply with a legal obligation.

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

For the purpose of processing and investigating your report and subject to the provisions of applicable local laws, the personal data you provide may be accessed, processed and used on a strictly need-to-know basis by

the relevant personnel of our organization, external advisors (e.g., legal advisors), or, in limited circumstances, by technical staff at GCS Compliance Services Europe Ltd. Co., trading as NAVEX with our written approval in order to provide technical support.

Personal data you provide may also be disclosed on a 'need to know' basis to specific law enforcement or regulatory authorities in order to comply with legal or regulatory requirements e.g., anti-money laundering regulation, or if we believe that disclosure is reasonably necessary to protect against fraud, or to protect our property or other rights or those of other users of the platform, third parties, or the public at large.

Data storage

We use NAVEX to store the personal data in databases located on servers in Frankfurt, Germany and Amsterdam, the Netherlands.

NAVEX prohibits unauthorized access or use of personal information stored on their servers. Such access is a violation of law, and NAVEX will fully investigate and take appropriate legal action against any party that has illegally accessed information within its systems.

Is your personal data safe and secure?

Strict technical and organizational measures are employed to protect your personal data from access by unauthorized persons and against unlawful processing, accidental loss, destruction, and damage both online and offline.

These measures include:

- training relevant staff to ensure they are aware of our privacy obligations when handling personal data
- administrative and technical controls to restrict access to personal data on a 'need to know' basis (roles and rights mechanisms, passwords)
- technical security measures (including fire walls, encryption and anti-virus software, monitoring of access, customer-specific controls, regular review of user accounts, regular back-ups etc.)
- incident management (strict procedures for incidents, bug fixing, personal data incidents and breaches, etc.)
- physical security measures, such as staff security badges to access our premises.

Although we use strict security measures once we have received your personal data, the transmission of data – especially over the internet – is never completely secure. Hence, we cannot guarantee the absolute security of data transmitted to us or by us.

NAVEX has implemented industry-accepted administrative, physical, and technology-based security measures to protect against loss, misuse, unauthorized access, and alteration of personal data in their systems. NAVEX ensures that any employee, contractor, corporation, organization, or vendor who has access to personal data in their systems is subject to legal and professional obligations to safeguard that personal data. See NAVEX's privacy notice here.

Cross border transfers

NAVEX is headquartered in the United Kingdom.

We have legal entities in APAC, EMEA, LATAM and NA. It is therefore possible that reports are received from those regions or personal data is transferred to recipients in those countries. User access is set up to ensure that personal data from the European Economic Area, the United Kingdom, or Switzerland, is not transferred outside the European Economic Area, United Kingdom, or Switzerland.

With regard to Zurich Cover More, an exception from this general user access applies for the purpose of assessing questions or reports regarding ethics and compliance in a consistent manner in the group by a Triage Committee based in NA (US).

For how long do we keep your personal data?

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 legal or financial requirements. In case judicial or disciplinary

proceedings are initiated, the personal data processed will be kept until those proceedings are definitively closed. We keep personal data to the extent permitted by law and our retention policies. Otherwise, we will delete or anonymize personal data that is no longer required, to the extent permitted by law.

Your rights

You have several rights, of which we would like to inform you; the right to access your personal data, the right of data rectification (if your personal data is inaccurate), the right of erasure (if the retention of your personal data is no longer necessary in relation to the envisaged purpose of the processing), the right to restrict the data processing (e.g., if you contest the accuracy of your personal data that we process), the right to data portability under certain circumstances and the right to lodge a complaint with the competent supervisory authority.

If you wish to exercise your rights mentioned above, please contact the respective subsidiaries' local privacy team or reach us by email at privacy@zurich.com.

Any ongoing investigation may limit or deny the rights listed herein. Documented reasons shall be provided if any of the listed rights are limited or denied. When access is granted to the personal data of any concerned individual, the personal data of the alleged wrongdoers, or third parties such as informants, whistleblowers or witnesses may be removed from the documents except in exceptional circumstances.