

Ethics and Compliance Helpline Privacy Notice

Scope and Overview

COOK (as set out in “Contact Us”) is committed to maintaining an ethical work environment by encouraging reports of suspected violations of law or company policies, as well as other concerns you may have, to COOK through a dedicated confidential helpline/platform (the “Helpline”), while also protecting the privacy and security of your personal data. This Notice applies to the personal data that we collect for the purposes of administering our program and investigating reports through the Helpline. The employees of COOK and external parties can use the Helpline to inform COOK about possible violations of legal requirements or internal regulations and thus contribute to their detection and prosecution. The data controller is as set out in “Contact Us” below, as applicable to the jurisdiction/COOK entity in connection with which you are reporting.

In certain countries, COOK may only accept reports through the Helpline that relate 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 COOK through the Helpline, you will need to contact your supervisor or local management or a representative of the Human Resources, Legal or Corporate Compliance Departments to report the matter. [You will be notified if this is the case.]

Other Data Privacy Notices apply to COOK’s collection of personal data outside of the context of the Helpline. For further information, please review COOK’s Privacy Notices available on our website <https://www.cookgroup.com/privacy-policy/> or contact your regional privacy team member using the contact information below.

Who Can Report?

The use of the Helpline is voluntary, and this Notice applies to all individuals who may report wrongdoing using the Helpline. This service is a confidential online reporting system that allows you to report suspected violations of law or company policies, as well as other concerns you may have, to COOK.

You will not be sanctioned for submitting information in good faith, even if it later turns out to be incorrect, but knowingly providing false or misleading information will not be tolerated.

Please note that, in accordance with applicable laws, individuals about whom an allegation is made or who are otherwise identified through a report submitted to the Helpline may be informed about the fact that a report has been made (but not about the identity of the person who made a report). In addition, all such individuals identified will have the right to respond to or correct the information you report.

Collection of Personal Data and Sensitive Personal Data

For purposes of this Notice, personal data means any information about an identifiable natural person but excludes anonymous data that is not associated with (and which does not identify) a particular individual.

When we receive allegations through the Helpline, we may collect, store, and process the following categories of personal data, which are required for us to investigate those allegations: (i) your name and contact details (unless you report anonymously) (ii) whether you are employed by COOK or if not, your relationship to COOK; (iii) 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); (iv) a description of the alleged misconduct as well as a description of the circumstances of the incident and (v) communications

data regarding use of COOK systems (including log and metadata) (vi) information provided by third parties during the investigation process (e.g., third party witnesses or other persons with relevant information pertaining to your report) (vii) any other information or documentation provided by the reporter.

The Helpline does not actively solicit sensitive or special categories of personal data (i.e., information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning sex life or sexual orientation), or information relating to criminal convictions and offences. However, it may prove relevant and necessary to collect such data in the context of particular allegations reported (e.g., when investigating a concern related to safety at work or discrimination).

Purpose and Lawful Basis for Processing of Personal Data and Sensitive Personal Data

We process personal data collected through the Helpline as necessary for the effective administration of our COOK's Ethics and Compliance program, reviewing the plausibility of reports, cooperating with any ombudspersons) and regulatory or legal authorities, to comply with our legal obligations, and to pursue COOK's legitimate interests in (i) investigating potential misconduct and other allegations brought to our attention, (ii) facilitating the reporting and raising of protected disclosures, ethical and/or legal concerns or non-compliance within COOK's business and the proper and fair investigation of such concerns and reports (iii) protecting the public against harm arising from dishonesty, malpractice, breaches of ethics or other improper conduct (including preventing future fraud, misconduct and business malpractice), (iv) reviewing relevance of reports and subsequent investigations for the wider COOK group, (v) complying with foreign legal regulations, (vi) clearing data subjects from incorrect accusations, (vii) improving COOK's compliance structures and (viii) the legal defence of COOK.

To the extent any sensitive or special categories of personal data are submitted by a reporter and/or otherwise collected, we will process this data only to the extent it is necessary and/or relevant for the purposes of administering our Ethics and Compliance program, investigating potential misconduct and the other purposes identified above. For example, processing of such sensitive personal data may be necessary:

- For carrying out our legal obligations and protecting rights under applicable employment, social security, and social protection laws.
- To establish, exercise, or defend legal claims.
- For reasons of substantial public interest (i.e., preventing or detecting unlawful acts, preventing, or detecting fraud, protecting the public).
- Where applicable to the extent that information relating to criminal convictions and offences is collected, in accordance with the laws of the jurisdiction authorising such processing and providing for appropriate safeguards for the rights and freedoms of the individual.

We will only process your personal data and sensitive personal data for the purposes for which we collected it unless applicable law permits or requires us to process your personal data for different purposes. If we need to process your personal data and/or sensitive personal data for purposes not identified above and which are not compatible with the original purpose for which the personal data was collected, we will do so only after providing you with appropriate notice and, if required by law, obtaining your consent.

You will not be subject to decisions based on automated data processing unless we have a lawful basis for doing so and we have notified you.

Information Shared

COOK limits access to personal data collected and processed as part of the Helpline on a need-to-know basis in connection with administering our Ethics and Compliance program and/or investigating potential misconduct or for the other purposes and interests set out in “Purpose and Lawful Basis for Processing of Personal Data and Sensitive Personal Data” above. COOK personnel are given access in accordance with their job role and responsibilities and are subject to appropriate confidentiality obligations.

We will only disclose your personal data to third parties where required by law or to parties who require the information to assist us with administering our Ethics and Compliance program, investigating potential misconduct or for the other purposes and interests set out in “Purpose and Lawful Basis for Processing of Personal Data and Sensitive Personal Data” above. Third-party service providers may include, but are not limited to:

- other companies within the COOK group, as necessary;
- third-party vendors, including NAVEX, the third-party vendor supporting the Helpline, and/or third-party service providers who implement security measures to protect your personal data consistent with our policies and any data security obligations applicable to us;
- third-party advisors such as outside legal counsel, consultants, auditors, and investigators, and (where applicable) external ombudspersons or works councils;
- third parties in respect of business transactions such as in the event of a transfer of ownership of our business;
- third parties as permitted or required by law, including in connection with regulatory or legal matters or where this is required for safety and security (for example, regulatory, governmental, court and law enforcement authorities).

When we share this information, we limit the transfer to the information that is necessary under the circumstances, we ensure appropriate security and take reasonable steps to comply with all legal requirements in respect of the transfer.

International Data Transfers

As a global organization, COOK stores data in secure, centralized systems as well as using service providers based globally. Accordingly, we may transfer the personal data we collect about you to other jurisdictions inside or outside the United States that may provide a different level of data protection. In accordance with applicable data protection laws, COOK has put in place appropriate measures to ensure an adequate level of protection for your personal data and applies those measures irrespective of where the data is processed or stored.

When we transfer your personal data out of the European Economic Area (EEA), Switzerland or the UK, we ensure an adequate level of protection by implementing one of the following safeguards:

- only transferring your personal data to a country or territory deemed to provide an adequate level of data protection by the European Commission and/or the UK supervisory authority; or
- by using specific data transfer contracts approved by the European Commission and/or the UK supervisory authority which give Personal Data the equivalent protection it has in Europe; or
- by using another approved lawful transfer mechanism.

Employees choosing to utilize the help line in the APAC region are encouraged to read and understand this Notice as your personal data associated with use of NAVEX may be securely transferred cross border. The personal data and information you provide through this helpline will be stored in a database which is located on servers hosted and operated in the United States by NAVEX. We contractually require our third-party service providers, like NAVEX, who act as data processors to implement appropriate security measures to protect your personal data consistent with our policies and any data security obligations applicable to us. For example, third-party service providers are not permitted to use your personal data for their own purposes and are only required to process your personal data for specified purposes in accordance with our instructions.

Data Security

COOK has put in place appropriate technical, physical, and administrative security measures to prevent unauthorized or unlawful disclosure or access to, or accidental or unlawful loss, destruction, alteration, or damage to the personal data that it collects. These measures are intended to ensure an appropriate level of security in relation to the risks inherent to the processing and the nature of the data to be protected and are applied in a manner consistent with applicable laws and regulations. COOK evaluates these measures on a continuing basis to help minimize risks from new security threats as they become known.

Data Retention

COOK retains your personal data for as long as necessary to fulfil the purposes COOK collected it for (as set out in “Purpose and Lawful Basis for Processing of Personal Data and Sensitive Personal Data” above), consistent with local law and business practices and deletes the personal data when it is no longer necessary and, in any case, upon expiration of the maximum storage term as set forth by applicable law, unless the personal data is required for a longer period, such as in the case of a claim, lawsuit or other regulatory investigation.

When assessing the data retention period, we consider the amount, nature, and sensitivity of the information, the potential risk of harm from unauthorized use or disclosure of the personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Individuals' Rights

Depending on your location and applicable laws, you may have the right to request access to, correct, or erase the personal data that we hold about you, restrict the processing of your personal data, or the right to data portability. You may also have the right to object to the processing of your personal data under certain circumstances. If you would like to make a request relating to the personal data, we hold about you in connection with the Helpline, please contact your regional data privacy contact as set out below.

These rights are not absolute and applicable law may allow or require us to deny your request. If we cannot comply to your request, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Individuals may also have the right to make a complaint at any time to their relevant supervisory authority for data protection issues. COOK would, however, appreciate the chance to deal with your concerns before you approach the relevant authority, so please contact us in the first instance.

Confidentiality/Non-Retaliation

If you are an employee, please refer to the COOK Code of Conduct and applicable policies for more detail on COOK’s confidentiality and non-retaliation practices.

Contact Us

<p>Europe</p>	<p>Email DataProtectionEurope@CookMedical.com</p> <p>Mail Address Cook Ireland Ltd. Attn: EU Data Protection Officer O'Halloran Road National Technological Park Castletroy, Limerick, Ireland</p>
<p>Asia-Pacific</p>	<p>Email DataProtectionAPAC@CookMedical.com</p> <p>APAC Mail Address COOK (China) Medical Trading Co Ltd Room1503, Ascendas Plaza, No. 333 TianYaoQiao Road, Shanghai 200030, China</p>
<p>United States or Other Locations</p>	<p>Email Privacy@CookGroup.com</p> <p>US Mail Address Cook Group Incorporated Attn: Chief Privacy Officer 750 Daniels Way, P.O. Box 1608 Bloomington, Indiana 47402-1608 USA</p>

Changes to this Notice

We reserve the right to update this Notice at any time and make it available on the website when we make any updates. If we would like to use your previously collected personal data for different purposes than those, we notified you about at the time of collection, we will provide you with notice and, where required by law, seek your consent, before using your personal data for a new or unrelated purpose. We may process your personal data without your knowledge or consent where permitted or required by applicable law or regulation.

Effective Date: [DATE]

