

Solenis Whistleblowing Privacy Notice

Introduction

Solenis company and its wholly and majority-owned entities (“**Solenis**”, “**Solenis Group**”, “**Company**”, “**we**”, “**our**” or “**us**”) takes your data protection seriously. This Whistleblowing Privacy Notice (“**Privacy Notice**”) has been issued for compliance with our obligations to provide individuals with information about the processing of personal data under applicable laws.

The purpose of this Privacy Notice is to inform you about the processing of personal data by Solenis as part of the reporting of concerns, potential or suspected misconduct, incidents, or events, through our **Share Your Concern** (whistleblowing) platform (the “**Reporting System**”).

Solenis is the controller in relation to the processing of personal data collected through the Reporting System. To this end, please note that the personal data in your report may be shared on a need-to-know basis within the Solenis Group, including (where relevant), with the Solenis entity that is your employer (if you are a Solenis employee), in order to properly investigate and resolve the issues reported.

The Reporting System is open to all Solenis employees and workers, consultants, officers, self-employed contractors, casual workers, volunteers, paid and unpaid trainees, agency workers and other Solenis stakeholders.

This Privacy Notice is supplementary to the [Solenis Privacy Statement](#) (and to the [Fair Processing Notice](#) in case you are Solenis employee) which provides information on how we process personal data of the data subjects referred to above. The content of the [Solenis Privacy Statement](#) (and the content of the [Fair Processing Notice](#) in case you are Solenis employee) applicable to these specific data subjects continues to apply to the Reporting System, in addition to the information set out in this Privacy Notice.

What information and personal data will be registered?

Reports

You can use the Reporting System to report suspected breaches of Solenis Business Code of Conduct, other policies and violations of the law including among other issues relating to conflicts of interests, bribery and corruption, competition law, fraud, financial crime, harassment and discrimination, protection of personal data, rights and protection of individuals or serious environmental damage or other misconduct of public interest.

Your personal data and sensitive personal data

In principle, the Reporting System can be used – to the extent permitted by law – without providing your personal data. You may, however, voluntarily disclose your personal data as part of the whistleblower process, in particular (a) information about your identity, e.g., your first and last name, your country of residence, your telephone number, or your email address; (b) a description of your concern, potential misconduct, a description of the incident or event you have witnessed / wish to report, and details of any personal opinion or expressions you may wish to make in connection with the incident or event; and (c) additional personal data may be generated and processed through the course of any investigation into the report.

The Reporting System is not intended to collect or process sensitive personal data, for example, information about an individual's race or ethnic origin, trade union membership, criminal charges, or convictions. Depending on the jurisdiction where you are located, additional categories of personal data may be treated

as sensitive. Due to free text fields in the reporting form, however, such sensitive personal data may be voluntarily disclosed by you. To the extent we receive sensitive personal data through the Reporting System, we will only process it in accordance with applicable law and this Privacy Notice for the purpose of investigating the allegations.

Personal data of persons concerned.

Personal data of persons mentioned in reports will be processed to the extent necessary to investigate and administer the reports. The categories of personal data that will be processed will vary from case to case and can include names, social security numbers, addresses, images, audio recordings, video material, employment numbers, gender, contact information and IP addresses. Sensitive personal data, such as information about health, ethnic origin, political and trade union affiliation, may also be processed. In some cases, information of suspected, alleged or proven criminal activity or offences, which is considered sensitive personal data, may be processed. Sensitive personal data are only processed for the purpose of investigating the report and are limited to what is strictly necessary for this purpose.

All personal data collected by the Reporting System will be managed confidentially and will only be disclosed as set out in this Privacy Notice.

Solenis recognizes that an individual may not wish to be identified during the course of raising a concern. In such circumstances, we will take appropriate measures to protect the identity of the person making the report and will not disclose it without their consent. If it proves impossible to resolve the matter without revealing the individual's identity, the investigation team dealing with the matter will discuss with them whether and how to proceed. In some cases, however, confidentiality cannot be absolutely guaranteed as the very fact of the investigation may serve to reveal the source of the information, the statement of the person raising the concern may be needed as part of evidence against the perpetrator, or legal proceedings may require the individual to appear as a witness.

Use of Personal Data and Sensitive Personal Data and the legal basis that apply

By using the Reporting System, you can get in touch with us and report any compliance or legal violations. We process your personal data in order to check the report you have made through the Reporting System and to investigate suspected compliance or legal violations, take appropriate action to address the concerns raised and prevent similar concerns from arising in the future. It may happen that we have questions for you. For this purpose, we will communicate with you through the Reporting System – unless you have given your explicit consent to another form of communication.

We only process personal data collected through the Reporting System as necessary for the administration of our whistleblowing program, to comply with our legal obligations, and to pursue our own legitimate interests in investigating potential misconduct.

To the extent we collect any sensitive personal data, we will process this data for the purpose of administering our program and investigating potential misconduct when the processing is necessary:

- In order to administer the report and investigate the reported circumstances.
- In order to take remedial measures following an investigation.
- In order to use reports as evidence in legal proceedings.
- For carrying out obligations and specific rights in the field of employment, social security and social protection laws.
- To protect an employee's or another person's vital interests.
- To establish, exercise, or defend legal claims.
- For reasons of substantial public interests.

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 (or sensitive personal data) for purposes not identified above, we will do so only after providing you with notice and, if required by law, obtaining your consent. We may process your personal data (or sensitive personal data) without your knowledge or consent, where permitted or required by applicable law or regulation.

The legal ground for processing of personal data in the local level reporting channels is legal obligation on Solenis under laws of various European countries, to have reporting channels and procedures.

Retention

Any personal data that is obviously not required for the administration of the report will be deleted as soon as possible. Personal data will be kept for as long as required to investigate the report, or, if applicable, as long as necessary to take any needed remedial measures. We may need to retain your personal data to exercise, establish or defend our legal rights (for example, in the event of a challenge or potential or actual litigation) or to comply with any relevant legal obligations. In any case, will only retain your personal data for as long as is reasonably necessary for the purposes for which it was collected and to comply with applicable laws and regulations.

Sharing personal data and cross-border transfer

Your information will be shared internally with Solenis staff in relevant departments so that we can handle, investigate, and respond to the concerns raised. This may include Human Resources, Finance, Business Advisory Services, Legal, Ethics and Compliance, and Management. Local level reports will be handled by designated persons authorized to receive and investigate reports at local level. Only such designated persons may have access to personal data while the report is being reviewed and investigated. Internal access to information processed as part of the investigation is granted to limited individuals on a need-to-know basis.

In certain situations, and depending on the subject matter and consequences of the report, we may need to share the information you send to us with third parties, such as external attorneys, government departments, enforcement agencies and the police. There may also be certain circumstances where we are required, by law, to share your information. We will notify you before we share your information unless such notification would hinder or obstruct investigation or actions to be taken regarding the reported circumstances.

Where permitted by applicable law, we may transfer the personal data to the United States and other jurisdictions that may provide a different level of data protection than your home country or country of employment, as necessary to administer our whistleblowing program or conduct an investigation. We have implemented contractual arrangements with the recipient of the personal data (e.g., Standard contractual clauses for data transfers between EU and non-EU countries, or other equivalent transfer mechanisms) to secure the transfer of your personal data to the United States and other jurisdictions. Depending on applicable laws, you may have a right to access these safeguards.

Your rights

Subject to certain exemptions as prescribed by applicable privacy laws or other applicable regulations, and in some cases dependent upon the processing activity we are undertaking, you have certain rights in relation to your personal data, such as - right of access, - rectification, - erasure, - to receive a copy of the personal data held in the Reporting System - restriction of processing, and, in certain cases, - the right to data portability. Furthermore, you have the right to object at any time, on grounds relating to your particular situation, to your personal data being processed. In addition, if you are the subject of the report, you may be able to correct personal data that is inaccurate or incomplete, or gain access to information concerning the report, except for the identity of the reporter. You may also receive notice if you are the subject of the report, except where doing so would threaten the integrity of the investigation. For more detailed information on your data protection rights, please read [Solenis Privacy Statement](#). You can exercise your rights by using the **Contact and complaints** section below.



While you may also have the right to lodge a complaint with the relevant data protection authority, we encourage you to contact us in the first instance, to resolve your concerns.

Data security

The reporting system is hosted by Lighthouse Services, Inc. an independent party guaranteeing the system's security and anonymity. Lighthouse Services, Inc. has taken the necessary technical and organizational measures to prevent personal data from being accidentally or unlawfully destroyed, lost or damaged and to prevent any unauthorized disclosure or misuse of the personal data. The processing of personal data is subject to strict controls and procedures and is in compliance with good practices in the field.

Contact and complaints.

We have appointed Office of Data Privacy (ODP) to oversee compliance with this Privacy Notice. If you have any questions, concerns or complaints regarding our compliance with this Privacy Notice, the information we hold about you within the Reporting System, or if you wish to exercise your rights, we encourage you to contact our ODP by sending an email to privacy@solenis.com, or by completing and submitting our [Data Request Form](#), or by using [Contact Us](#) section of our website.

We will investigate and attempt to resolve complaints and disputes and make every reasonable effort to honor your wish to exercise your rights as quickly as possible and, in any event, within the timescales provided by applicable laws.

Changes to the Privacy Statement

We occasionally update this Privacy Notice, if we change our business processes or if there are legal changes required.

We may amend this Privacy Notice from time to time to keep it up to date with legal requirements and the way we operate our business. Please regularly check our web page or Intranet for the latest version of this Privacy Notice.

Last update: September 2024