

Infinera Global Whistleblowing Privacy Notice

Last updated: April 4, 2024

1. Introduction

Infinera Corporation, with its principal place of business located at 6373 San Ignacio Avenue, San Jose, CA 95119, USA ("**Infinera Corporation**") and its subsidiaries, affiliates, and related entities (collectively referred to as "Infinera", "we", "us" or "our") have implemented a Code of Business Conduct and Ethics and relevant policies for the purpose of complying with federal, state, and local laws and regulations, including EU Directive 2019/1937 on "the protection of persons who report violations of Union law" as transposed into national laws applicable to Infinera entities (hereinafter collectively referred to as the "**Whistleblowing Law**"). If you wish to contact Infinera regarding your personal data or concerns you have about this privacy notice, please contact us at DataPrivacy@infinera.com.

This privacy notice explains how personal data of individuals filing a report or mentioned in the same will be processed for the management of the reports and relevant investigations, in accordance with the Infinera Whistleblowing Policy, available here <https://www.infinera.com/whistleblower-policy> ("**Policy**"), and the Whistleblowing Law. For more information on Infinera's Whistleblowing Reporting channels (including Infinera's ethics and compliance hotline), how to submit a report, and the rules that apply to using the reporting line, please review the Policy and information on how to report a violation available here: <https://www.infinera.com/report-a-violation/>.

This privacy notice supplements Infinera's employee privacy notices applicable to our employees in different jurisdictions, which apply to Infinera's collection of personal data outside of the whistleblowing context. For further information on how we process employees' personal data other than through our Whistleblowing Reporting channels, please refer to our employee privacy notice applicable to you.

2. Who is responsible for processing the data?

We will collect and process personal data of individuals involved in the reports (i.e. reporting party, reported party, witnesses, facilitators and any natural person involved in a report) as data controller or joint controllers, if applicable under the Regulation (EU) 2016/679 ("**GDPR**", together with other applicable data protection laws, "**Privacy Laws**").

Near the end of this privacy notice are specific disclosures for individuals located in Italy. If you are located in Italy, please also review the section near the end of this notice that pertains to your jurisdiction.

3. Which categories of personal data may be processed?

The following categories of personal data may be processed:

- identity, function, location of work/incident and contact details (e.g., first and last name, verification credentials, identification number, job title, work address, phone number, email address) of the reporting person - if not anonymous;
- identity, function, location of work/incident and contact details of the persons subject of the reporting;

- identity, function and contact details of the persons involved in the processing of the facts reported;
- personal data contained in (i) the facts reported, (ii) communications and other information collected and reviewed in connection with the reporting and the subsequent investigation of the facts reported, and in (iii) the investigation report; and
- personal data contained in information pertaining to the outcome and consequences of the investigation of the facts reported.

Your provision of personal data as a person making the report is voluntary. Failing to provide personal data as well as filing an anonymous report may delay or make it impossible for Infinera to act upon any report you submit.

4. What are the purposes of data processing?

We process personal data in reports to manage, investigate and take appropriate action in response to the reports according to Whistleblowing Laws, Policy and to establish, exercise and defend legal claims in this context.

5. What are the legal bases for data processing?

We rely on the following legal bases for the data processing herein described:

- Infinera's legitimate interests to investigate and take appropriate action related to a potential violation of the Code of Business Conduct and Ethics and relevant policies, their procedures or other matters as described in the Policy, thereby ensuring compliance and to establish, exercise or defend legal claims in this context. Failure to pursue these legitimate interests may have severe consequences for Infinera.
- The processing is necessary to protect vital interests of those who file a report or are the subject of a report;
- The processing is necessary for Infinera to comply with legal obligations;
- Your consent. The identity of the reporting person and any other information from which that identity may be inferred, directly or indirectly, may not be disclosed, without the express consent of the reporting person, to persons other than those responsible for receiving or following up on the reports, who are expressly authorised by Infinera to process such data. Express consent is also required when using the voice messaging channel or recording in person meetings.

6. Is the information kept confidential and whom do we share personal information with?

Personal data may be accessed by:

- Infinera's authorized personnel subject to a specific duty of confidentiality;
- Infinera's service providers (such as Navex Inc. who offers the reporting channel platform), who will act as data processors, duly appointed and instructed on the basis of a specific contract. An updated list of such processors is available by contacting us as described below.

- Competent law enforcement authorities who will act as independent controllers as allowed by applicable laws.

The identity of a person making a good faith report and the information related to the report will be kept confidential and will not be disclosed to third parties other than the processors mentioned above. However, the following exceptions apply:

- if sharing the person's identity is necessary for the correct processing of the report or to carry out further investigation or take measures in light of the investigation; or
- if disclosing the person's identity is necessary by law (which may include to respond to a request by a regulator to know the identity, provided that we are legally obliged to comply with such a request).

You should not include in reports special categories of personal data (except where necessary due to the nature of the report), untruthful information, or personal data that is unnecessary for the investigation. If we receive such information, we will delete such information promptly except as necessary to investigate abuse of the Infinera Whistleblowing Reporting channels.

7. Will personal data be transferred to third parties and abroad?

Infinera operates across the globe, and we may transfer your personal data in your home jurisdiction or other jurisdictions only for the purpose of data processing described in this privacy notice. If you are located in the EU and the data recipients are established in third countries without an adequate level of protection of personal data, we will take all necessary measures to ensure that the transfer of data outside the EU is adequately protected as required by applicable Privacy Laws, including using the European Commission's Standard Contractual Clauses, application of the additional contractual, organizational and technical measures required and monitoring the standards adopted by these service providers with regard to the protection of personal data and security.

For a list of countries where we transfer personal data please see Appendix I. You may obtain more information on these safeguards by contacting us at the contact details indicated below.

8. How long is personal data retained?

Any information collected as a result of a report will be kept only as long as necessary and for the purpose for which it has been collected in compliance with applicable law, as detailed below.

Personal data relating to reports giving rise to an investigation will be deleted or anonymized once no longer necessary for the investigation and usually no longer than 5 years (unless longer period is permitted or required by applicable law or regulation) from the date of communication of the outcome of the reporting procedure. However, in case of further legal proceedings such as disciplinary actions or the investigation of criminal proceedings, personal data will be kept until the end of such proceeding, including potential periods of appeal, and will then be deleted or archived as permitted by applicable law. Transcripts of interviews and communications may only be kept for the time strictly necessary and proportionate to the investigation.

As noted at Section 6 above, certain personal data that is not relevant to an investigation will be promptly deleted except as necessary to investigate abuse of the Infinera Whistleblowing Reporting channels.

9. Rights with respect to Personal Data

Individuals (such as any reporting person or person subject to a report) have a number of rights in relation to the personal data processed as described in this privacy notice, including the right to obtain confirmation of the existence of personal data; verify its content, origin and accuracy, requesting its integration, updating, amendment, deletion or transformation into anonymous form, portability, limitation. **Under certain circumstances individuals have the right to object, on grounds relating to their particular situation, at any time to the processing of their personal data.**

You may at any time revoke your consent as applicable under the laws and lodge a complaint with the applicable data protection supervisory authority in your country.

Please note that exercising these rights is subject to certain requirements and conditions as set forth in applicable law. In any event, these rights may be delayed, limited or excluded, for as long as and to the extent that this constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the data subject, in order to safeguard the duty of confidentiality pursuant to Whistleblowing Law and Privacy Laws.

If you wish to exercise these rights, obtain an updated list of data processors, obtain further information on transfers to third countries, or obtain Infinera's legitimate interest assessment, you can contact us at DataPrivacy@infinera.com

10. Updates to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with or publish a new privacy notice when we make any substantial updates.

11. Jurisdiction-Specific Disclosures

Italy

Infinera Corporation and Infinera S.r.l., with registered address at Via Messina 38, 20154 Milan, Italy ("**Infinera S.r.l.**" and jointly referred to with Infinera Corporation as the "**Joint Controllers**"), process personal data of individuals involved in the reports as joint controllers under GDPR.

According to Art. 26 GDPR, Infinera Corporation and Infinera S.r.l. have entered into a joint controllership agreement to establish their respective obligations in data processing activities aimed at the management of reports. For more information, you can contact the Joint Controllers as below indicated.

DataPrivacy@infinera.com

You may at any time revoke your consent related to data processing under this privacy notice, as applicable, and lodge a complaint with the Italian privacy authority (Garante per la protezione dei dati personali, www.garanteprivacy.it).

If you wish to exercise your rights under this privacy notice, you can contact the Joint Controllers at DataPrivacy@infinera.com. You may also exercise your rights through the Italian Data Protection Authority as specified in the Privacy Laws.

Appendix I

List of countries for transfer of personal data

United States

United Kingdom

Germany

Portugal

Sweden

Canada

Brazil

Mexico

India

China

Philippines

Singapore