Analog Devices Inc. Whistleblowing Notice

1. Introduction

This Whistleblowing Notice is to help you understand what personal data we collect about you, why we collect it, and how we use it in relation to our global whistleblowing hotline portal.

2. Anonymous reporting

You may choose to report anonymously, but we encourage you not to do so. Including your identity and contact information may allow us to obtain more information or follow up with you directly regarding your concerns. If you provide your identity and contact information, we will strive to keep your identity confidential. However, some EU countries do not allow us to keep your identity confidential, such as in case of access requests by other individuals.

3. Controller

Analog Devices Inc. (**ADI**), is responsible for the processing of your personal data in relation to our global hotline portal.

If you are in the EEA, the controller for the processing of your personal data may be one of our subsidiaries in the EU (**ADEU**). A list of our global subsidiary list may change, and the current list can be found on the subsidiary exhibit of Analog Devices Inc.'s 10-K form, searchable from here). If, in view of the report, we decide to share the personal data with ADI, ADEU and ADI are joint controllers for the processing of the personal data in the context of your whistleblowing report(s).

Our EU Data Processing Officer is Nicole Jahn, Nicole.Jahn@analog.com, and our primary business address is Analog Devices International U.C. Bay F-1 Raheen Industrial Estate Limerick, Ireland.

If you are in the People's Republic of China, the personal information handler for the processing of your personal data is Grace Lin, and her primary business address is Human Resources, Analog Devices (China) Holdings Co., Ltd., Unit 1107, 222 Hubin Road, Huangpu District, Shanghai, China, PRC (200021).

If you have any questions relating to the use of your personal data or if you would like to receive more information on the processing of your personal data in the context of our whistleblowing portal, please contact us via dataprivacy@analog.com.

Types of personal data collected and the purpose and the applicable legal basis

Your personal data is (i) provided by you; and/or (ii) created by us when handling your report.

We may collect, store, and use your personal data as set out in the "personal data" column below. You will also find the purpose of the processing and the legal basis we rely upon below.

Personal data	Purposes	Legal basis
Report data, such as the name of the organization, country, city, and location of the violation, your country, relationship with Analog Devices, the nature, location,	• Maintain and manage our global whistleblower hotline portal.	**EEA** Necessary for the purposes of our legitimate interests (Article 6(1)(f) GDPR) namely, to ensure compliance with our Code of Business Conduct and

Personal data	Purposes	Legal basis
occurrence, and timeframe of the incident, when and how you became aware, and any other information in the report and its attachments. *Contact data (optional),* such as your first and last name, phone number, email address, and availability. *Allegation data,* such as the first and last name and title of the person engaged in the behavior, of the witness(es), and of the supervisor or manager(s) involved. *Other data,* such as your log-in details to the platform.	• Ensure compliance with our Code of Business Conduct and Ethics. • Ensure a safe and secure work environment.	Ethics and to ensure a safe and secure work environment. **PRC** Necessary for the implementation of human resources management in accordance with the legally formulated labor rules and regulations and the legally concluded employment contracts (Article 13(2) of the Personal Information Protection Law of the People's Republic of China (**PIPL**)).

4. Location and sharing of your personal data

Your personal data is stored and accessed in the United States.

Navex, the provider of our global whistleblowing hotline portal, stores the personal data on its systems. We have a written agreement in place with Navex describing and limiting how they can use the data. This agreement complies with the requirements of the GDPR.

Your information will be processed for the purpose of reviewing and responding to your report and will not be shared unless required by applicable laws or necessary to review, process, or take action relating to your report.

Where necessary we share your personal data with local authorities. We will do so in compliance with applicable laws and regulations, in particular if we share your personal data with authorities outside the country where you are located.

If we share your personal data with our ADI subsidiary, affiliate companies, or third parties, we take steps to ensure (i) compliance with the local applicable laws and regulations and (ii) that appropriate safeguards are in place to guarantee the continued protection of your personal data. In particular if the personal data processing is covered by the GDPR and in the absence of a European Commission's adequacy decision, we may do so by signing the Standard Contractual Clauses adopted by the European Commission (article 46(2)(c) GDPR). For more information on the Standard Contractual Clauses, please see here. If the personal data processing is covered by the PIPL we may do so by (i) conducting a personal information protection impact assessment and (ii) entering into standard contracts as required under the PIPL.

5. Retention

We do not retain your personal data longer than needed for the processing purpose. Our standard retention period for personal data relating to whistleblowing reports is 10 years from the date the investigation and/or related corrective actions were finally resolved. Notwithstanding the above, we will retain your personal data if we need to do so for the establishment, exercise or defense of legal claims. Likewise, we will retain your personal data to make it available to competent supervisory

authorities, investigative authorities, courts, or other governmental bodies as required or permitted by law.

6. Your rights

Depending on your location, you may have various rights relating to your personal data. These may include: the right to access your personal data, the right to have your personal data rectified or erased, the right to restriction of the processing, the right to data portability and the right to object to the processing on grounds relating to your particular situation. Most of these rights are not absolute and are subject to exemptions in the GDPR and/or other local applicable laws and regulations, including the PIPL. If you would like to exercise a data right regarding your data, you may contact dataprivacy@analog.com.

We will strive to respond to your exercise of right request within one month and have the right to extend this period to two months. If we extend the response period, we will let you know within one month of your request.

In addition, you have the right to lodge a complaint with a supervisory authority in the country of your residence, where you work or where an alleged infringement of the applicable data protection law took place. A list of EU supervisory authorities and their contact details is available here.