Privacy Notice

1. Introduction

This Privacy Notice ("**Notice**") applies to the ABB Group of companies, which means ABB Asea Brown Boveri Ltd and each entity in which ABB Asea Brown Boveri Ltd, directly or indirectly, has a majority holding or owns or controls the majority of voting rights, including its subsidiary companies. The ABB affiliate conducting an internal investigation together with or on behalf of ABB Ltd, Switzerland and ABB B.V., Netherlands as joint controllers (referred to as "**ABB**" or "**we**"), are responsible for the processing of your personal data and other information related to you in the context of an investigation, and controls how it is used, in accordance with this Notice.

ABB is fully committed to protecting your privacy and respecting your rights to control how your personal data is used. This notice explains why and how the ABB Integrity Investigations and Monitoring Team and any other investigative instance at ABB that is entrusted with conducting internal investigations (**"ABB Investigators"**) may collect and use your personal data for conducting investigations and the rights you have in relation to that data if your personal data is collected or used for this purpose. We take the privacy of your personal information seriously and we aim at ensuring highest standards for protection of whistleblowers in line with EU law and local legislations.

For the avoidance of doubt, as noted on our Business Ethics Helpline platform, ABB does not collect personal data to identify reporters to the Helpline. Our Business Ethics Helpline does not generate or maintain any internal connection logs with IP addresses, so no information linking a reporter's PC or other electronic device is available to ABB.

If you are a reporter, please be aware that the information you provide or the allegations that you make could result in decisions that affect employees of ABB and other third parties involved in the matter. We therefore kindly ask you to provide us only with information that is in good faith and is accurate to the best of your knowledge. Please do not provide us with any information if doing so could violate applicable laws of your country.

2. Who is responsible for the processing of your personal data?

Processing of personal data is held by ABB Group of companies and operationally managed by:

ABB B.V. George Hintzenweg 81 Rotterdam 3068 AX Netherlands

When it comes to subsidiary companies, they can share resources with its parent company provided that the person / Integrity team at headquarters level would be authorized to access the report for the purpose of carrying out necessary

investigation. You, as a reporting person, have a right to object to that and to request that the reported conduct is only investigated at the level of the subsidiary.

Other subsidiary companies of ABB may also receive and process your personal data, either in the capacity of controller or processor and this Notice applies equally to them.

For purposes of conducting internal investigations, we may obtain your personal data from you, from existing ABB managed data sources, from external third-party data providers (including personal data reported through the ABB Business Ethics Helpline), or from publicly available data sources accessible to everyone.

3. The types of information we collect and use

Integrity investigations are conducted to determine whether ABB's Code of Conduct, other ABB policies or the law have been violated. In the course of conducting integrity or other internal investigations, we may collect and use personal data that concerns you in connection with the activity that is subject to investigation, which may be reported by you or someone else (including anonymous reporters where permitted by law). We may collect the following categories of personal data:

- **Identification data and business contact information** such as first name, last name, nickname, job/position/title, business email address, business address, business telephone number, business mobile number, telefax number, private telephone number, personal mobile number, personal email address, digital alias/signature, date of birth, Customer or Consumer ID.
- **Personal data related to family and social circumstances** such as gender, age, marital and family status (including also the name and contact details of the next of kin).
- **Employment related personal data** such as employee number, signature, employment status, social security and tax numbers, country of residence, nationality, photo, emergency contacts and passport information, work and residence permit, immigration status and travel visa information, badge card information.
- **Qualifications** such as records of education and work achievements including current and previous positions, education and training courses, background check, resume/CV, in some cases: contact details of referees and results of capability assessments and interview assessment/feedback.
- **Job information and work metrics** such as position, title, employment contract, line manager, job band, performance history, employment status, leave or absence information, working time logging, training records, performance targets, development goals, professional feedback.
- **Compensation, allowances, benefits and expense related information** such as salary data, payroll data, pension plan number and contributions, non- salary benefits, bonus, compensation, share options, dependents, beneficiaries or health benefit nomination, bank statements, expense claims and receipts, bank account details, credit card data, phone expenses and insurance data.
- **Financial and other details** such as account information, credit checks, payment details and transactions, investigation information and disciplinary history.
- **Electronic identification data and information collected by the communications systems, IT applications and website browser** such as information technology usage (system access, IT and internet usage), device identifier (mobile device ID, IP address, browser type, browser settings, time and URL accessed), registration and login credentials, login data and log files, analytics ID, searches, website registration and sound recordings (e.g. voice mail/phone recordings, Microsoft Teams, Zoom or similar

recordings), posts by individuals in discussions/social media like Yammer, etc.

- **Other personal data (which may include special categories of information as mentioned below)** such as business documents containing personal information (e.g., queries, questions, complaints, orders and related records; emails; reports; contracts; presentations, minutes; work products), itemized telephone bill, photos, images and/or videos.
- **Additional information provided to us by you, a reporter, a witness or third party in the course of an investigation.** Please provide us only with information that is in good faith and is accurate to the best of your knowledge. Please do not provide us with any information if doing so could violate applicable laws of your country.

The below mentioned types of personal data are only collected and processed, if at all, in accordance with applicable local laws in your country of residence.

Special categories of personal data such as:

- membership of religious congregations;
- health and medical information, including disability status, special working conditions (such as use of a standing desk) and medical devices needed on the premises, work related injury and illness information, data for travel emergency support (blood type, medical history, allergies);
- race or ethnicity;
- in some cases: trade union membership, and sex life or sexual orientation, political opinions (e.g., where this is used for investigations of non-equal treatment).

- **Data about criminal convictions and offences** such as criminal background information and sanction list information to the extent required for the purposes of criminal background screening and Know Your Customer ("KYC") or Anti Money Laundering ("AML") or whistleblowing legislations obligations.
- **To the extent necessary to fulfil our obligations, data obtained from publicly accessible sources or which are legitimately transmitted by other third parties (e.g., a credit agency)** such as data in public professional social media (e.g. LinkedIn), background check data.

Requests to be provided with information about a specific personal data processing activity can be made that by submitting a request at **www.abb.com/privacy.** Such requests will be considered in light of ABB's legal obligations and rights you may have.

4. Why we use your personal data?

While conducting internal investigations, we use personal data as listed above for the following purposes:

・To detect, prevent, investigate and remediate violations of ABB's Code of Conduct, policies and the law;

・Otherwise protect legal rights (including liaison with regulators and law enforcement agencies for these purposes);

- Otherwise reduce financial, legal and reputational risks to the organization.

We use your personal data in whistleblowers case management process in case you raise concern or in case your personal data will be reported in a concern that was raised by another person. ABB established a complaint reporting mechanism allowing whistleblowers to report their concerns that also protects against retaliation and implemented case management process that keeps the data confidential.

In order to achieve this purpose, ABB Investigators review allegations that come in through the ABB Business Ethics Helpline, or are otherwise raised through any other reporting channel, and by doing so review personal data of involved parties. Personal data is shared onwards beyond the investigative teams if and as appropriate to achieve these purposes.

We only collect the personal data that we need for these purposes.

5. The legal basis we rely on

We rely on our **legitimate interests** to process your personal data insofar as this is not overridden by your own privacy interests. Such interests may include:

- investigating and ensuring compliance with legal, regulatory, and ABB internal requirements and policies, including ABB's Code of Conduct;
- prevention of fraud and criminal activity including through the review, investigation and monitoring of reports and indicators of such activity, the misuse of ABB assets, products and services, and as strictly necessary and proportionate for ensuring network and information security; and
- transmitting personal data within the ABB group for internal administrative purposes as necessary, for example to provide centralized services.

Without processing of personal data for internal investigations and monitoring purposes ABB might be exposed to legal claims, threats to the company's reputation and culture, and/or imposed to financial loss.

You may obtain a copy of our assessment regarding our legitimate interest to process your personal data by submitting a request at www.abb.com/privacy.

With regard to special categories of personal data (information on: racial or ethnic origin or trade union membership or religious and philosophical beliefs or health data or sex life or sexual orientation or political opinions) that may be included in a concern raised by you to any ABB reporting channel or ABB Investigator, we ask you to give consent for processing it in a content of your report. If you raise a complaint and do not consent to ABB processing relating data, ABB cannot take further action. In such case, we will remove all sensitive personal data that was related to you unless there is another legal justification to keep it.

With regard to special categories of personal data we will only process such data in accordance with applicable law and:

- with your explicit consent for specific activities in accordance with applicable law;

- where necessary for establishment, exercise and defense of legal claims;
- when necessary for exercising rights based on employment, social security or social protection law or as authorized by collective agreement; or
- with regard to personal data concerning criminal convictions and offences, we will only process such data where such processing is permitted by applicable (local) law.

6. Parties we share your personal data with

We only share your personal data with other ABB affiliates or third parties as necessary for the purposes described in this Notice. Where we share your personal data with an affiliate or third party so that it is transferred to or becomes accessible from outside the European Union ("EU") and the European Economic Area ("EEA") or outside the country where the ABB company that controls your data is located, we always put adequate safeguards in place to protect your personal data. Examples of these safeguards are an adequacy decision of the European Commission or Standard Contractual Clauses. We have taken additional measures for the transfer of data from within to outside the EU, EEA and outside the country where the ABB company that controls your data is located to protect your personal data. If you would like an overview of the safeguards which are in place, please submit a request at www.abb.com/privacy.

Recipient category	Recipient location	Purpose
ABB affiliates and subsidiaries	See the list of ABB subsidiaries EU/EEA and non-EU/EEA (global)	The purposes described in section 4, including steps required to investigate and remediate alleged integrity violations.
Contact center	Intake point: Canada Servers: Ireland, the Netherlands	Intake and translation of integrity reports; storage of data.
Service providers such as IT services, and other	Depending on situation:	Depending on reporting channel and investigation process-
service providers working on ABB's behalf	EU/EEA and non-EU/EEA (global)	IT services, investigative service providers, due diligence service providers, forensic service providers, and legal service providers.

7. How long we keep your personal data

Based on mandatory legislation, ABB must keep certain personal data for a minimum period of time. We only keep your personal data for as long as necessary for the purposes described in this privacy notice.

In order to fulfill the purpose of our processes, ABB Investigators often rely on their own records as a tool for obtaining information on parties who have appeared in previous cases. ABB Investigators are also responsible for providing integrity related information on employees and business partners for re-employment and due diligence checks. We only store your personal data for the time necessary for conducting investigations and undertaking necessary actions.

Your personal data might be kept for longer period only if required by local laws and regulatory requirements. At the same time, applicable data protection laws require that we do not keep personal data in an identifiable form for any longer than is necessary for the purpose for which the personal data is being processed. Through the setting of IT applications and policies we ensure that your personal data is deleted when we no longer need it.

8. Security and monitoring of ABB systems and sites

ABB takes the security of its data very seriously, including your information and ABB's digital business assets. ABB sees this as a shared responsibility, where it takes the necessary steps to secure such data, and where it expects its staff members to do the same. You can read more about our security measures and your responsibilities End User Security Policy.

9. Which data protection rights do you have with regards to your personal data

Depending on the jurisdiction in which you are located and in which your personal data is processed, you may also have the right to:

- access your data - you are entitled to ask ABB for an overview of or to obtain a copy of the personal data we hold about you;
- have your data corrected - you may request immediate correction of inaccurate or incomplete personal data we hold about you;
- have your data erased - you may request that personal data be erased when it is no longer needed, where applicable law obliges us to delete the data or the processing of it is unlawful;
- restrict data processing - can request to restrict processing of your personal data in specific circumstances;
- port your data - you have a right to receive a copy of your data in a structured, commonly used and machine-readable format for your own purposes, or to request us to transfer it to a third party;
- object to data processing - You have the right to object at any time, for reasons arising from your particular situation, to the processing of your personal data, which is based a legitimate interest.
- consent withdrawal - you may withdraw your consent at any time. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

Please note that the rights described above are not absolute, and that your request cannot always be met entirely. For example, sometimes we cannot delete or restrict the processing of your personal data as we may have legal obligations or contractual obligations to keep certain personal data.

You may request to enforce your data privacy rights at www.abb.com/privacy.

10. Contact and further information

If you want to access your personal data, make use of any of your other rights mentioned above or if you have any questions or concerns about how ABB processes your personal data, please contact our Group Data Protection Officer at privacy@abb.com, or submit your complaint at www.abb.com/privacy.

Should you not be satisfied with our response or believe we are processing your personal data against the law, you may also have the right to file a complaint with the Data Privacy Authority in your country of residence or work, or seek a remedy through the courts where you believe an infringement of data privacy laws may have taken place.