ABB Ability™ Data Privacy Policy

Scope and purpose
At ABB, respecting data privacy is a top priority. This ABB Ability™ Data Privacy Policy ("**Ability DPP**") applies to our processing of personal data in connection with our provision and our customer's use of ABB Ability™ services, software and/or related access to an ABB portal or mobile application and when it is referenced, e.g. in the ABB Ability™ General Terms and Conditions.

This Ability DPP explains (i) why and how we collect personal data; (ii) how we process such data; and (iii) what rights individuals have regarding their personal data. This Ability DPP is not a privacy notice aimed at an individual whose personal data is being collected and processed as part of an ABB Ability service and/or related access to an ABB portal or mobile application. We will provide individuals with separate privacy notices where and when required. In addition, if an individual is accessing the abb.com website or any associated website, the abb.com Privacy and Cookies Policy (https://new.abb.com/privacy-policy), as amended from time to time, applies.

Certain ABB Ability™ related business transactions may require the processing of personal data beyond the scope of this Ability DPP. In such cases the processing of personal data may require the conclusion of additional data processing/protection agreements. A party shall, upon request of the other party, promptly enter into any such agreement(s) as required by mandatory law or a competent data protection authority.

Who controls personal data
The ABB entity that entered into an agreement with a customer entity or such other ABB entity which is providing services or is communicating with a customer entity is responsible for the personal data. For applicable data protection law, such ABB entity will be the controller of the personal data. Each such entity is regarded as an independent controller of the personal data, and this Ability DPP applies to all such companies.

The personal data we collect and how we get it
We collect the following categories of personal data:

- **The business contact information shared with us:** name, title, job title, email address, business address, telephone number, mobile telephone number
- **Additional information provided to us in the course of our business relations, such as:** interests in ABB products, marketing preferences, registration and login information, audit logs, contract or order data, invoices, payments, credit card or other payment information, business partner history, etc.
- **Information a browser makes available when an individual visits an ABB website or an ABB mobile application:** IP address, the source of the site visit, time spent on the website or a particular page, links clicked, comments shared, browser type, date and time of visit, etc.

What we may use personal data for
Depending on our product and service delivery we may use the personal data to:

- process and fulfill orders and keep an individual informed about the status of an order;
- provide and administer our services, software and products;
- provide customer support and process, evaluate and respond to requests and inquiries;
- conduct and facilitate customer satisfaction surveys; and
- perform data analytics (such as market research, trend analysis, financial analysis, and customer segmentation).

We only collect the personal data that we need for the above purposes. We may also anonymize the personal data, so it no longer identifies an individual and use it for various purposes, including the improvement of our services, software and products and testing our IT systems.

The legal basis on which we use personal data
We use the personal data for the purposes described in this Ability DPP based on one of the following legal bases, as applicable:

- We may process the personal data for the fulfilment of contractual obligations resulting from contracts, or as part of pre-contractual measures;
- We may process the personal data on the basis of statutory requirements, for example, on the basis of tax or reporting obligations, cooperation obligations with authorities or statutory retention periods; or
- We will rely on our legitimate interests to process the personal data within the scope of a business relationship. Our legitimate interests to collect and use the personal data for this purpose are management and furtherance of our business.

How we share personal data
We only share the personal data with other ABB affiliates or third parties as necessary for the purposes described in this Ability DPP. Where we share the personal data with a party outside of the EU, we always put safeguards in place to protect the personal data as described below.

Recipient name or – for non-EU countries – recipient category	**Recipient location**	**Purpose**	**Safeguards in place to protect your personal data**
ABB affiliates and subsidiaries	See the list of ABB subsidiaries	The purposes described in this Ability DPP	EU Model Clauses
ABB business partners, distributors, and agents	EU and non-EU	The purposes described in this Ability DPP	EU Model Clauses
Service providers and subcontractors	EU and non-EU	IT services, payment processors, customer support and other services providers working on ABB's behalf	EU Model Clauses and commercial contracts ensuring the data is only used to provide the services to ABB
Potential or actual acquirers of ABB businesses or assets	EU and non-EU	For the evaluation of the business or assets in question or for the purposes described in this Ability DPP	EU Model Clauses and commercial contracts ensuring the data is only used to evaluate ABB's business or assets or for the purposes described herein
Recipients as required by applicable law or legal process, to law enforcement or government authorities, etc.	EU and non-EU	Where required by applicable law or a legitimate request by government authorities, or a valid legal requirement	We will ensure, to the extent possible, that adequate protection is provided for the data when it is transferred out of the EU in these circumstances

How long we keep personal data
We only keep the personal data for as long as necessary for the purposes described in this Ability DPP. After this time, we will securely delete the personal data, unless we are required to keep it in order to meet legal or regulatory obligations, or to resolve potential disputes.

Technical and organizational security measures

We take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of personal data and we restrict access to personal data to ABB employees who need to have that information in order to fulfill their respective tasks in accordance with the customer contract and this Ability DPP. We will in particular take the following measures to protect the personal data if and when appropriate.

Access control and pseudonymization

- Physical access controls to prevent unauthorized access to data processing facilities, e.g.: entry protected by magnetic or chip cards, keys, biometric controls, facility security services and/or entrance security staff, alarm systems, video/CCTV systems;
- Logical and data access controls to prevent
    - unauthorized use of the data processing and data storage systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, multi-factor authentication, encryption of data at rest and transit; and
    - unauthorized reading, copying, changes or deletions of data within the system, e.g. rights authorization concept, need-to-know based access, logging and storing of system access events;
- Segregation of data to isolate processing of data, which is collected for different purposes, e.g. multiple controller support, sandboxing;
- Pseudonymisation to process personal data in such a method/way, that the data cannot be associated with a specific data subject without the assistance of additional information.

Integrity

- Data transfer control to prevent unauthorized changes or deletion of data within network or physical transfer or transport, e.g.: digital signing, write-only file systems or media;
- Data entry controls to verify by whom personal data is entered into a, is changed in or deleted, from a data processing system e.g.: logging and storing of transactions.

Availability and resilience

- Availability controls to prevent accidental or willful destruction or loss, e.g.: backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), malware protection, threat, vulnerability and patch management, firewall, reporting procedures and contingency planning;
- Rapid recovery, e.g. Disaster Recovery Strategy and Processes.

Procedures for regular testing, assessment and evaluation

- Data protection management, incident response management, intrusion detection and protection, data protection by design and default;
- Order or contract controls, e.g.: clear and unambiguous contractual arrangements, formalized instruction management, strict controls on the selection of third parties, duty of pre-evaluation, supervisory follow-up checks.