Data Privacy Policy

Contents

1. Introduction 1

2. Relationship to other legal provisions and national law 3

3. Privacy Principles 3

4. Data Processor Principles 8

5. Data Security 9

6. Sharing Personal Data with Third Parties 9

7. Records of processing 10

8. Data Privacy Organisation 10

9. Training 11

10. Monitoring Compliance 12

Appendix 1 13

Privacy Risk Assessment and Privacy Impact Assessment Procedure 13

Appendix 2 14

Third Party Personal Data Transfer Policy 14

Appendix 3 17

Data Subject Rights Policy 17

1. Introduction

1.1. Key Terms

The terms used in this Privacy Policy are defined as follows:

ABB means the ABB corporate group of companies.

Audit Conditions means that the person auditing will be independent and appropriately qualified, comply with ABB's security and confidentiality requirements; that the audit will be conducted during business hours; and that, unless the person responsible for the audit has reasonable grounds to believe that there is a material breach of applicable data protection Law, the audit will take place no more than once in any year and will take place on at least 30 days' notice.

Competent Supervisory Authority means any other supervisory authority which is 'concerned' by the processing of Personal Data because (i) [ABB Entity] is established in the country or territory in which that supervisory authority is established; (ii) because Data Subjects living in the country or territory of that supervisory authority are likely to be affected by [ABB Entity]'s processing of Personal Data, or (iii) it has received a complaint from a Data Subject relating to processing of Personal Data by [ABB Entity].

Country Privacy Lead means the person who is appointed in accordance with national law to be the local data protection officer (where required by local law) or the local data privacy contact. They are responsible for monitoring data privacy compliance in their country or cluster of countries. This person is the contact person to the Group Data Protection Officer.

Customer means a person which has entered into an agreement with [ABB Entity], where [ABB Entity] processes Personal Data on behalf of, and pursuant to the instructions of the Customer.

Data Controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data.

Data Processor means the natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the Data Controller.

Data Subject means the individual to whom Personal Data relates.

Employee means any person who has an employment contract with [ABB Entity].

EU Model Clauses means the clauses resulting from the EU Commission Decisions dated 24 December 2004 (2004/915/CE) and 5 February 2010 (2010/87/UE).

European Law means (a) for European Personal Data to which the GDPR or Directive (EU) 2016/680 applies, or which have been transferred from the European Union, any law of the European Union or of a Member State of the European Union transposing that Directive or enacting provisions associated with the GDPR or which otherwise contain rules relating to the processing of Personal Data; and (b) for European Personal Data to which the data protection laws of Norway, Iceland, Liechtenstein or the United Kingdom (once the United Kingdom has ceased to be an European Union Member State) apply, or which have been transferred from that country, the laws of that country all as amended or replaced from time to time. In each case, such laws must provide appropriate safeguards for the rights and freedoms of Data Subjects.

European Personal Data means Personal Data which is processed by [ABB Entity] and to which European Law applies.

GDPR means Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation).

Group Data Protection Officer means the person responsible for monitoring data privacy compliance at a group level.

Member State means a member state of the European Union.

Personal Data means any information relating to an identified or identifiable individual ('Data Subject').

Sensitive Personal Data means special categories of Personal Data that reveal the individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person and data concerning health, sex life or sexual orientation.

Sub-processor means an entity appointed by a Data Processor to process Personal Data, with the approval of the Data Controller.

Third Party means any person or entity (e.g. company, organisation or government authority) which is not part of ABB.

1.2. Scope

This Privacy Policy applies to the processing of all Personal Data by [ABB Entity], regardless of where the data is collected and irrespective of the competent jurisdiction applicable to the processing.

2. Relationship to other legal provisions and national law

2.1. The highest data protection standards will prevail

The principles described in this Privacy Policy shall be respected by [ABB Entity] irrespective of local laws, except:

- where such local laws provide more stringent requirements (in which case, such local laws shall continue to apply in addition to this Privacy Policy);
- or where GDPR permits a derogation or exception in EU or Member State Law.

2.2. Requests from law enforcement and state security bodies

Where a legal requirement to transfer Personal Data conflicts with EU or national laws restricting cross-border data transfer, any relevant transfer of Personal Data requires the approval of the Group Data Protection Officer.

3. Privacy Principles

[ABB Entity] must meet the privacy principles below whenever they process Personal Data for ABB's purposes - that is, when ABB is the Data Controller for the Personal Data.

3.1. Ensure processing of Personal Data is fair and lawful

Always process Personal Data fairly and lawfully and on the basis of one of the following grounds for processing:

- the Data Subject has given their consent to the processing in accordance with Section 3.8;
- the processing is necessary to perform a contract with the Data Subject, or to take steps at the request of the Data Subject before entering into a contract;
- the processing is necessary for compliance with a legal obligation to which the Data Controller is subject;
- the processing is necessary to protect the vital interests of the Data Subject; or
- the processing is necessary for the Data Controller's legitimate interests or those of a third party, unless the interests of the Data Subject override those interests.

If Employees of [ABB Entity] are unclear when beginning any new Personal Data processing about whether there is a valid legal basis for the processing, they must contact their Country Privacy Lead.

3.2. Process Special Categories of Personal Data fairly and lawfully

The Country Privacy Lead must be consulted prior to the processing of Sensitive Personal Data.

Only process Sensitive Personal Data if one of the following grounds for processing applies:

- the Data Subject has given explicit consent in accordance with Section 3.8 (unless EU or other national law provides that the Data Subject may not provide consent);
- the processing is necessary to meet obligations or exercise rights in national laws (if the Sensitive Personal Data is European Personal Data, rights in European laws) relating to employment, social security and social protection;
- the Personal Data are manifestly made public by the Data Subject;
- the processing is necessary to establish, exercise or defend legal claims; or
- the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the Employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of national law (if the Sensitive Personal Data is European Personal Data, on the basis of EU or Member State law) or pursuant to contract with a health professional and subject to applicable law.

The treatment of Personal Data about criminal convictions and offences will vary between jurisdictions: only process such Personal Data where the processing is authorised by applicable law.

3.3. Use Personal Data for limited purposes

Only process Personal Data for explicit and legitimate purposes which are specified (a) to the Data Subject as part of the Transparency Principle (see Section 3.7); and (b) in the records of processing (see Section 7).

Do not process Personal Data for any incompatible purpose - unless the Data Subject has given consent and you have provided the information required by the Transparency Principle (see Section 3.7), or the processing is permitted under applicable law.

3.4. Use limited, quality Personal Data

Make sure Personal Data are adequate and relevant to the purposes of processing. Make sure the Personal Data are limited to what is necessary to the purpose of processing.

Make sure Personal Data are accurate and, where necessary, kept up to date. Take all reasonable steps to ensure that any incorrect or incomplete Personal Data is erased, blocked or, if necessary, corrected without delay.

3.5. Keep Personal Data only for as long as necessary

Only keep Personal Data for the period necessary for the purposes for which they are processed, or as advisable considering an applicable statute of limitations. At the end of this period erase the Personal Data or ensure that the data does not allow Data Subjects to be identified unless there is an exemption under applicable law which allows the data to be kept for longer. Comply with ABB's Policy on Records Management, found on the Group Charter Portal, and applicable local records management policies and procedures.

3.6. Data Protection by Design and Default

Ensure that data protection is considered from the beginning of each project involving new processing of Personal Data or where [ABB Entity] intends to merge with or acquire another company. Ensure that appropriate technical and organisational measures and safeguards are built into the project to implement the privacy principles and protect the rights of Data Subjects.

Complete a privacy risk assessment for each project involving new processing of Personal Data according to the process set out in Appendix 1 (Privacy Risk Assessment and Privacy Impact Assessment Procedure) so that appropriate technical and organisational measures and safeguards can be applied to the processing.

Before undertaking any processing of Personal Data which is likely to result in a high risk (as determined by the risk assessment built into the Privacy Management tool) to the rights and freedoms of Data Subjects, carry out a data protection impact assessment in accordance with the process set out in Appendix 1 (Privacy Risk Assessment and Privacy Impact Assessment Procedure).

3.7. Be transparent to Data Subjects

Always process Personal Data in a manner which is transparent to the Data Subject and provide Data Subjects with the following information ('privacy notice'):

- the identity and the contact details of the Data Controller;
- contact details of the Data Controller's data privacy officer, where one has been appointed;
- if an EU representative has been appointed under Art. 27 of the GDPR, the identity and contact details of the representative;
- the purposes for which the Personal Data will be processed;
- the legal basis for each purpose for which Personal Data are processed;
- where the legal basis relied on is legitimate interests, details of the particular interest;
- the recipients, or categories of recipients, of the Personal Data;

- any international data transfers, including information as to how the Personal Data will be protected (where the Personal Data is European Personal Data, as required by Art. 13(1)(f) & Art 14(1)(f) of the GDPR);
- retention periods for the Personal Data, or if that is not possible, the criteria used to determine the retention period;
- information about data subject rights to access, portability, rectification, erasure and restriction, objection to processing, to withdraw consent and to complain to a supervisory authority;
- where [ABB Entity] will use automated decision-making which has legal or similarly significant effect, this must be explained, together with meaningful information about the logic involved and the consequences of the processing for the Data Subject; and
- where the Data Subject must provide Personal Data because this is required by law, or is necessary for a contract, this must be explained – as well as the consequences of not providing the Personal Data.

When Personal Data are collected directly from the Data Subject, provide this information when the Personal Data are collected.

If the Personal Data is not obtained directly from the Data Subject, you must also provide the following information:

- the categories of Personal Data processed; and
- the source of the Personal Data and if this was a publicly accessible source.

If Personal Data are not obtained from the Data Subject, provide this information:

- within a reasonable period after obtaining the Personal Data, but at the latest within one month;
- if [ABB Entity] will use the Personal Data to communicate with the Data Subject, at the time of the first communication with the Data Subject; or
- if [ABB Entity] intends to disclose the Personal Data to others, at the time when the Personal Data are disclosed.

If the purposes for processing Personal Data change, provide a further privacy notice before the new processing takes place.

Ensure privacy notices are concise, understandable and use clear and plain language, which is suitable for the audience.

Ensure privacy notices are easily accessible. Provide the privacy notice in writing (which can include electronic means), unless the Data Subject asks for the information to be provided orally.

[ABB Entity] does not have to provide a privacy notice if:

- the Data Subject is already aware of the information;
- [ABB Entity] has obtained the Personal Data from someone other than the Data Subject and it would be impossible to provide the information, or would involve disproportionate effort; or
- another exemption applies under applicable law.

Consult the Country Privacy Lead before relying on one of these exemptions.

Use the template information notice found in the ABB Privacy Management tool to ensure you meet these requirements.

3.8. Consent

Obtain specific, informed, clear and freely given consent prior to beginning any processing of Personal Data where consent is required or relied on as the legal basis for processing. Consent for processing of Sensitive Personal Data must be explicit and clearly refer to the processing of the specific category of Sensitive Personal Data.

Do not rely on consent where there is a clear imbalance of power between the Data Subject and [ABB Entity]; you should look for another legal basis for processing.

Consent should only be obtained where Data Subjects have a genuine choice over whether [ABB Entity] can use their personal data for the purpose described. For processing of Personal Data in the employment context, the legal basis cannot and should not be the consent of the employees, due to the nature of the relationship between employer and employee.

To obtain valid consent, you must:

- obtain separate consents for each processing activity;
- keep records of obtained consents and withdrawals;
- allow Data Subjects to provide their consent in an easily accessible written format and to just as easily withdraw that consent;
- obtain declarations of consent which are precise, clear, in plain language and distinguishable from other matters presented to the Data Subjects at the same time; and
- inform Data Subjects that they can withdraw their consent at any time and explain the effects of withdrawing consent on earlier processing at the same time as obtaining the consent.

Always consult the relevant Country Privacy Lead (or the Global Data Privacy Officer for global projects) to determine whether consent is an appropriate legal basis. If you rely on consent, use the Template Consent Form found in the ABB Privacy Management tool and always consult your Country Privacy Lead (or the Global Data Privacy Officer for global projects) when drafting a Consent Form to ensure you meet these requirements; otherwise the consent will be invalid.

3.9. Respect data subject rights

Whenever [ABB Entity] processes European Personal Data as a Data Controller, comply with valid requests from Data Subjects to access or port their Personal Data; to rectify it; to erase or restrict the Personal Data; and to object to certain processing of their Personal Data, all as further set out in Appendix 3 (Data Subject Rights Policy). Whenever [ABB Entity] processes non-European Personal Data as a Data Controller, comply with valid requests from data subjects to enforce the rights available to them under applicable law and (if applicable) the relevant Country Data Protection Directive.

Do not use entirely automated processing of Personal Data to take decisions that will significantly affect the Data Subject unless the rules in Appendix 3 (Data Subject Rights Policy) are followed.

4. Data Processor Principles

When [ABB Entity] processes Personal Data as a Data Processor, on behalf of a Customer which is the Data Controller, [ABB Entity] must co-operate and assist the Customer, in a reasonable time and to the extent reasonably possible, to comply with its obligations under applicable law. This includes assisting with the privacy principles below:

- **transparency, fairness and lawfulness**: provide reasonable help and assistance to the Customer to comply with transparency, fairness and lawfulness;
- **purpose limitation**: process the Personal Data only on behalf of the Customer and in compliance with the Customer's documented instructions and in accordance with the contract with the Customer;
- **control of sub-processors**: following the Customer's instructions includes:
    - giving the Customer authority to decide whether [ABB Entity] can appoint a sub-processor;
    - providing the Customer with information on the main elements of the sub-processing (the parties, countries, security and onward transfer provisions); and
    - if requested, providing the Customer with a copy of the data protection provisions in the sub-processing contract;
- **storage limitation:** at the end of provision of the services to the Customer, at the Customer's choice, return the Personal Data to the Customer or delete the Personal Data and all copies of the data and certify to the Customer that this has been done;
- **data quality and storage retention:** at the Customer's request, implement necessary measures:
    - to update, correct or delete Personal Data and, where applicable, given the nature of the data processing, inform any approved Sub-processor;
    - to delete or anonymised the Personal Data once use in identifiable form is no longer necessary and where applicable, given the nature of the data processing, inform any approved Sub-processor;
- **security, privacy by design and by default, personal data breaches and data protection impact assessments:** assist the Customer to meet its obligations in this regard (as set out in the GDPR and applicable national law), taking into account the nature of the processing and the information available to [ABB Entity]; and
- **individual rights:** at the Customer's request, execute any necessary measures (taking into account the nature of the processing and in so far as this is possible) to fulfil Customer's obligation to meet Data Subject rights where relevant under applicable law – for example, communicating useful information to help the Customer to comply. Forward any request received from a Data Subject, in respect of whom the Customer is the Data Controller, to the Customer without answering it unless a different approach is agreed with the Customer.

When [ABB Entity] acts as a Data Processor on behalf of a Customer, it should ensure there is a written contract with Customer Data Controller, which is recognised as valid under applicable law and which contains the provisions set out in Parts B and C of Appendix 2 (Third Party Personal Data Transfer Policy).

5. Data Security

[ABB Entity] must implement appropriate technical and organisational measures to ensure a level of appropriate security for Personal Data, taking into account:

- risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data;
- the ability to ensure confidentiality, integrity, availability and resilience of processing of Personal Data;
- the need to test and evaluate the effectiveness of the technical and organisational measures;
- the requirements of applicable law which applies to the Controller of the Personal Data; and
- any measures specified in the service agreement or data processing agreement with a Customer where the Customer is the Controller of the Personal Data.

[ABB Entity] must comply with the information security requirements set out in ABB's Information Security Management Group Directives, Group Instructions, Policies and Standards (see the Overview of the Information Security Management System and its Documents).

Where a [ABB Entity] becomes aware of a personal data breach, it must follow the procedures set out in the InfoSec Be Secure Guide.

6. Sharing Personal Data with Third Parties

6.1. Sharing data with Data Processors and Sub-Processors

[ABB Entity] may only appoint a Data Processor to process Personal Data where a data protection and information security risk assessment has been carried out in accordance with the applicable Supply Chain Management and/or Information Security guidelines to determine that the Data Processor will provide sufficient guarantees that it will implement appropriate technical and organisational measures.

[ABB Entity] must ensure that there is a written contract with the Data Processor, which is recognised as valid under applicable law and which contains the provisions set out in Part A of Appendix 2 (Third Party Personal Data Transfer Policy).

Where a Sub-processor is appointed by [ABB Entity] to process Personal Data for which a Customer is the Data Controller, then the additional provisions set out at Section 4 above apply and provisions set out in Part C of Appendix 2 (Third Party Personal Data Transfer Policy), must be included in the contract with the Sub-processor.

6.2. Sharing Personal Data with Data Controllers

[ABB Entity] may share Personal Data with another Data Controller where:

- ABB is the Data Controller in respect of the Personal Data; and
- it meets the Privacy Principles at section 3 above, including being able to justify the sharing as set out at sections 3.1 and 3.2 above.

6.3. Onward transfer of European Personal Data

European Personal Data may be shared with ABB Group Companies or Third Parties in the European Union or located in a country or territory in respect of which there is a valid decision by the European Commission determining that such country, territory, or sector in a country ensures an adequate level of protection for European Personal Data in accordance with this Privacy Policy. In this case, no further contractual requirements to ensure adequate protection for the data are necessary.

In all other situations, European Personal Data may only be shared where appropriate safeguards are put in place, as set out in Art. 46 of the GDPR – such as use of the EU Model Clauses.

Where [ABB Entity] is the Data Controller in respect of the European Personal Data, then European Personal Data may also be shared in specific situations where European Law provides a derogation for the transfer – for example, where the Data Subject has given explicit consent or where the transfer is necessary to perform a contract with the Data Subject, or to take pre-contractual measures requested by the Data Subject. Always consult your Country Privacy Lead before relying on one of these derogations.

6.4. Onward transfer of non-European Personal Data

Non-European Personal Data may only be shared with other entities where appropriate safeguards have been put in place to protect the data and in accordance with the requirements of applicable law.

7. Records of processing

[ABB Entity] must be able to demonstrate compliance with this Privacy Policy.

As part of demonstrating compliance (in addition to the requirements set out in sections 8-10 below), [ABB Entity] must:

- keep a record of its processing of Personal Data using the ABB Privacy Management tool, which may be made available to a Competent Supervisory Authority on request, and which must include the name and contact details for [ABB Entity], details of any transfers of Personal Data outside the European Union and a general description of the security measures in place, and:
    - where [ABB Entity] is a Data Controller, disclose the categories of Personal Data processed, the categories of Data Subject, the purposes of processing, the categories of recipients to whom Personal Data will be disclosed and the retention periods for the data; or
    - where [ABB Entity] is a Data Processor, disclose the name and contact details of each Data Controller and its data protection officer (where one is appointed), the categories of processing carried out, and the retention periods for the data.

8. Data Privacy Organisation

[ABB Entity] must appoint a data protection officer if this is required by the GDPR or if this is required by an applicable national law.

8.1. Group Data Protection Officer

ABB has appointed a Group Data Protection Officer who is responsible for:

- monitoring and annually reporting on data privacy compliance at the highest management level and ensuring compliance with this Privacy Policy;
- implementing training, informing and advising ABB Companies on data protection matters (including involvement in data protection impact assessments) in global projects;
- cooperating with and acting as the point of contact for Supervisory Authorities and handling their investigations;
- handling complaints from individuals received at group level; and
- supporting Country Privacy Leads.

8.2. Country Privacy Leads

The Group Data Protection Officer is supported by Country Privacy Leads, whose role is to:

- monitor data privacy compliance and training in their country or cluster of countries;
- establish local organisation for supporting the implementation of this policy;
- advise on local data protection matters;
- be the primary point of contact for Data Subjects in their country or cluster;
- handle local complaints from Data Subjects;
- monitoring local legal requirements and updating the Group Data Protection Officer as necessary in accordance with Section 2; and
- report major privacy issues to the Group Data Protection Officer.

8.3. Privacy Management Team

The Privacy Management Team is the primary point of contact for all employees and external individuals that require management of their personal data held by ABB. The Privacy Management Team's role is to:

- manage the interactions with these individuals;
- manage the requests across the company from receipt to response including any changes needed in the appropriate systems; and
- own and manage the Privacy Management tool/system.

9. Training

ABB shall provide training on this Privacy Policy and other privacy and data security obligations to all Employees. Specific training shall be provided to Employees who have: permanent or regular access to Personal Data; responsibilities associated with managing processing of Personal Data; or who are involved in the development or procurement of products, services or tools used to process Personal Data.

Attendance to the data protection training (delivered globally as e-learning) will be monitored through the Group Legal & Integrity Department, assisted by the Country Privacy Leads where necessary.

10. Monitoring Compliance

[ABB Entity] shall audit business processes which involve the processing of Personal Data for compliance with this Privacy Policy. Such audits shall be carried out regularly during Group Internal Audit's usual activities on behalf of [ABB Entity] and at the request of the Global Data Protection Officer. The audit will be undertaken either by Group Internal Audit or appropriately qualified external auditors. [ABB Entity] shall take adequate steps to remedy breaches of this Privacy Policy identified during monitoring or auditing of compliance.

[ABB Entity] will provide copies of the results of any audit to a Competent Supervisory Authority and will agree to audits by a Competent Supervisory Authority in accordance with the Audit Conditions.

Appendix 1

Privacy Risk Assessment and Privacy Impact Assessment Procedure

Employees who develop new projects involving Personal Data processing shall complete a privacy risk assessment using the ABB Privacy Management tool. The results of each privacy risk assessment shall be provided to the relevant Country Privacy Lead or the Global Data Privacy Officer (where the project is global) and the results shall be recorded in the Records of Processing.

Where the privacy risk assessment indicates a high risk to Data Subjects, a data protection impact assessment must be completed, with the involvement of the relevant Country Privacy Lead or the Global Data Privacy Officer (as appropriate).

Data protection impact assessments will include a description of the processing activities and their purpose and an assessment of the need for and proportionality of the processing, the risks arising and measures adopted to mitigate those risks, in particular safeguards and security measures to protect Personal Data. Where a data protection impact assessment is required (see above), the template will be sent to the relevant business owner from the Privacy Management tool. The business owner will need to complete the template with the assistance of the relevant Country Privacy Lead (or the Global Data Privacy Officer in case it is a global project).

Where the data protection impact assessment indicates a high and unmitigated risk to Data Subjects, [ABB Entity] must consult with the Competent Supervisory Authority in conjunction with the Global Data Privacy Officer.

Appendix 2

Third Party Personal Data Transfer Policy

Part A: Terms to be included in contracts with Data Processors

Nature of processing to be described	✓	subject matter and duration of processing
	✓	nature and purpose of processing
	✓	type of personal data
	✓	categories of data subjects
	✓	obligations and rights of ABB/the end customer
Purpose limitation	✓	Data Processor may only process personal data on clear, documented instructions
Data transfer	✓	Data Processor may only transfer the data outside the EU, or, for data originating from Norway, Iceland, Liechtenstein, Switzerland and the United Kingdom (once the United Kingdom has ceased to be part of the EU), outside that country if instructed to do so by ABB o exception possible if the Data Processor is subject to European Law which requires the personal data to be transferred; notify the Data Controller of this unless that European Law imposes secrecy requirements on important public interest grounds
Confidentiality for Personnel	✓	All personnel authorised to process the personal data to be bound by confidentiality obligations
Security	✓	Description of the technical and organisational measures to protect personal data
Sub-processing	✓	Authorisation required to appoint sub-processors o If general authorisation is given, inform the Customer of changes so as to allow ABB to object (which may be met by providing a right to terminate)
	✓	Flow down substantially similar obligations to the Sub-processor.
	✓	Liability for acts of the Sub-Processor
Data Subject rights	✓	Assist the Data Controller in responding to these – so far as is possible and taking into account the nature of the processing
Personal data breaches	✓	Assist the Data Controller in managing its obligations in relation to personal data breaches under GDPR and other applicable law, taking into account the nature of the processing and the information available to the Processor
	✓	Report personal data breaches to the Data Controller without undue delay
Data Privacy Impact Assessments (DPIAs)	✓	Assist the Data Controller in conducing data protection impact assessments and consulting with the competent supervisory authority, taking into account the nature of the processing and the information available to the Processor
Storage limitation	✓	Return or delete personal data at the end of the services, at the Data Controller's choice, and delete all copies of the personal data o Exception possible if retention required by applicable law
General assistance	✓	Make available all information necessary for the Data Controller to demonstrate it has met its obligations (under Art.28 GDPR) in appointing and managing a Data Processor
	✓	Notify the Data Controller if, in the Data Processor's opinion, an instruction infringes applicable law and European Law in particular
Audit	✓	Allow and contribute to audits, including on-site inspections, conducted by the Data Controller or an auditor nominated by Data Controller

Part B: Terms to be included only in contracts with Customers where ABB acts as Data Processor

Topic	Requirement
Customer to inform Data Subjects	✓ If Sensitive Personal Data will be transferred, Customer must commit to inform Data Subjects that this data will be transferred to a third country ✓ Customer to inform Data Subjects that it uses Data Processors not in European Countries (if applicable)

Part C: Terms to be included in contracts with Customers and in Contracts with Sub-Processors

Topic	Requirement
Nature of processing to be described	✓ subject matter and duration of processing ✓ nature and purpose of processing ✓ type of personal data ✓ categories of data subjects ✓ obligations and rights of the Customer
Purpose limitation	✓ only process personal data on clear, documented instructions
Data transfer	✓ only transfer the data outside the EU, or, for data originating from Norway, Iceland, Liechtenstein, Switzerland and the United Kingdom (once the United Kingdom has ceased to be part of the EU), outside that country if instructed to do so by the Customer o exception possible if ABB is subject to European Law which requires the personal data to be transferred; notify the Customer of this unless that European Law imposes secrecy requirements on important public interest grounds
Confidentiality for staff	✓ All staff authorised to process the personal data to be bound by confidentiality obligations
Security	✓ Description of the technical and organisational measures to protect personal data ✓ May be provided via link

Sub-processing	✓ Customer authorisation required to appoint sub-processors, whether part of ABB or external o If general authorisation is given, inform the Customer of changes in a timely manner so as to allow Customer to object (which may be met by providing a right to terminate) ✓ Flow down substantially similar obligations to the Sub-processor. The obligations are those: o Relevant to the processing by the Sub-processor in the services agreement with the Customer o Set out in this Appendix 3 Part B (including purpose limitation, acceptance of audit, duty to assist with data subject rights and queries from supervisory authorities, and with DPIAs, storage limitation, rules on appointment of sub-processors) o Duty to assist the Customer (Privacy Policy, section 4) ✓ Liability for acts of the Sub-processor
Data Subject rights	✓ Assist the Customer in responding to these – so far as is possible and taking into account the nature of the processing
Personal data breaches	✓ Assist the Customer in managing its obligations in relation to personal data breaches under GDPR and other applicable laws, taking into account the nature of the processing and the information available to the Processor ✓ Report personal data breaches to the Customer without undue delay
DPIAs	✓ Assist the Customer in conducing data protection impact assessments and consulting with the competent supervisory authority, taking into account the nature of the processing and the information available to the Processor
Storage limitation	✓ Return or delete personal data at the end of the services, at the Customer's choice, and delete all copies of the personal data o Exception possible if retention required by European Law
General assistance	✓ Make available all information necessary for the Customer to demonstrate it has met its obligations (under Art.28 GDPR) in appointing and managing a Data Processor ✓ Notify the Customer if, in the Data Processor's opinion, an instruction infringes European Law or other applicable law of which the Data Processor is aware
Audit	✓ Allow and contribute to audits, including on-site inspections, conducted by the Customer or an auditor nominated by Customer o Those auditing must follow the Audit Conditions

Appendix 3

Data Subject Rights Policy

Rights of Data Subjects

Whenever [ABB Entity] processes European Personal Data, it must respond to requests from Data Subjects, as set out below. Whenever handling Data Subject requests, always use clear and plain language, appropriate to the Data Subject; provide information, without undue delay and in any event within one month of receipt of the request, on the steps taken in response to the request and, if a request has not been met, explain why to the Data Subject and advise the Data Subject of their right to complain to a supervisory authority or the courts.

Rights of access and portability:

1. Confirm if [ABB Entity] processes Personal Data about that Data Subject.

2. Provide a copy of the Personal Data in commonly used electronic form.

3. Provide supporting explanatory materials as set out in Art. 15(1) (a) – (h) and Art. 15(2) of the GDPR.

4. Provide the Personal Data to the Data Subject, or, at the Data Subject's request, to another entity, in a structured, machine-readable format where the Personal Data was provided by the Data Subject, is processed automatically, and where the Personal Data are processed with the individual's consent or to fulfil a contract with him or her.

Right of rectification:

Comply with valid requests from Data Subject to rectify inaccurate Personal Data, without delay.

Right of erasure (the "right to be forgotten"):

1. Comply with valid requests from Data Subjects for their Personal Data to be "erased" without undue delay - when there is a problem with the underlying legality of the processing, or where the processing was based on consent and they withdraw this consent. If the Data Subject asks, tell him or her whether you have disclosed his or her Personal Data to others – and notify them of the erasure, unless this proves impossible or would involve disproportionate effort.

2. If [ABB Entity] has made the Data Subject's Personal Data public, take reasonable steps to inform other Controllers which are processing the Personal Data, that the Data Subject has requested erasure.

Right of restriction:

1. Comply with valid requests from Data Subjects to "restrict" processing of Personal Data whilst complaints (about accuracy, lawfulness or objections to processing) are resolved, or if the processing is unlawful but the Data Subject objects to erasure and prefers restriction instead.

2. Whilst a request to "restrict" Personal Data is in place, store the Personal Data but do not otherwise process such data, unless the Data Subject gives consent or the data must be processed to establish, exercise or defend legal claims or to protect the rights of another

person, or for reasons of important public interest recognised in European Law. Notify the Data Subject before lifting the restriction.

3. If the Data Subject asks, tell him or her whether you have disclosed his or her Personal Data to others – and notify them of the erasure, unless this proves impossible or would involve disproportionate effort.

Right to object:

Comply with valid requests from Data Subjects to object to: (i) processing for direct marketing purposes, including profiling for purposes of direct marketing; (ii) processing justified on legitimate interests; and (iii) processing for scientific or historical research purposes or statistical purposes.

Automated decision-taking:

Do not take decisions solely on the basis of automated processing of Personal Data of a Data Subject (i.e. no human involvement in the decision) which produce legal effects, or have similarly significant effects, unless permitted by, and in line with any safeguards required by, European Law and after consulting the relevant Country Privacy Lead.