
	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	1 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

I. TABLE OF CONTENTS

I.	TABLE OF CONTENTS.....	1
II.	INTRODUCTION AND OBJECTIVES	2
III.	SCOPE OF APPLICATION	2
IV.	REFERENCE:.....	2
V.	KEY TERMS AND ABBREVIATIONS:.....	2
VI.	PROCESS DEFINITION	4
1.	RELATIONSHIP TO OTHER LEGAL PROVISIONS AND NATIONAL LAW	4
2.	PRIVACY PRINCIPLES	4
3.	DATA PROCESSOR PRINCIPLES	8
4.	DATA SECURITY	9
5.	SHARING PERSONAL DATA WITH THIRD PARTIES.....	10
6.	RECORDS OF PROCESSING	11
7.	DATA PRIVACY ORGANISATION	11
8.	TRAINING.....	12
9.	MONITORING COMPLIANCE.....	13
10.	VIDEO SURVEILLANCE POLICY	13
11.	DATA PRIVACY GUIDANCE	13
VII.	ENCLOSURES.....	14
I.	APPENDIX 1	14
1.	PRIVACY RISK ASSESSMENT AND PRIVACY IMPACT ASSESSMENT PROCEDURE	14
II.	APPENDIX 2.....	15
1.	THIRD PARTY PERSONAL DATA TRANSFER POLICY	15
III.	APPENDIX 3.....	19
1.	DATA SUBJECT RIGHTS POLICY.....	19
IV.	APPENDIX 4.....	21
1.	COMPANY VIDEO SURVEILLANCE POLICY.....	21
V.	REVISION HISTORY	26
VI.	FINAL PROVISIONS.....	26

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	2 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	No previous document		

II. INTRODUCTION AND OBJECTIVES

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

III. SCOPE OF APPLICATION

The provisions of this instruction are applicable at all ABB units/companies in Bulgaria. ABB Bulgaria EOOD, a sole owner limited liability company organized and existing under the laws of the Republic of Bulgaria, registered in the Commercial Register with the Registry Agency, Uniform Identification Code 831133152, having its registered seat and address at: 89B, Vitosha Boulevard, Building A, Floor 17, Sofia 1408, Triaditsa District, Republic of Bulgaria (hereinafter referred to as “**Company**” or “**ABB in Bulgaria**”)


IV. REFERENCE:

- General Data Protection Regulation (EU) 2016/679
- For country specific questions, please contact your [ABB Bulgaria Country Privacy Lead \(CPL\)](#).
- For Function specific questions, please contact the dedicated [GDPR Function Leads](#).
- Link to Bulgarian [Data Protection Commission \(www.cdpd.bg\)](http://www.cdpd.bg).


V. KEY TERMS AND ABBREVIATIONS:

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) Company 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 Company's processing of Personal Data, or (iii) it has received a complaint from a Data Subject relating to processing of Personal Data by Company.
- **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 Company, where Company processes Personal Data on behalf of, and pursuant to the instructions of the Customer.

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	3 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

- **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 Company.
- **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 Company 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').
- **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration.
- **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, organization or government authority) which is not part of ABB.

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	4 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

All definitions of GDPR apply to this Country Policy, unless the context requires otherwise.

VI. PROCESS DEFINITION

1. Relationship to other legal provisions and national law

1.1. The highest data protection standards will prevail

The principles described in this Privacy Policy shall be respected by Company 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.

1.2. 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.

2. Privacy Principles

Company 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.

2.1. 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 2.8;
- 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 Company 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.

2.2. 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:

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	5 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

- the Data Subject has given explicit consent in accordance with Section 2.8 (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.

2.3. 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 2.7); and (b) in the records of processing (see Section 6).

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 2.7), or the processing is permitted under applicable law.

2.4. 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.

2.5. 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.

2.6. 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 Company intends to merge with or acquire another

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	6 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

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).

2.7. 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 Company 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.

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	7 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

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 Company will use the Personal Data to communicate with the Data Subject, at the time of the first communication with the Data Subject; or
- if Company 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.

Company does not have to provide a privacy notice if:

- the Data Subject is already aware of the information;
- Company 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.

2.8.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 Company; you should look for another legal basis for processing.

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	8 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

Consent should only be obtained where Data Subjects have a genuine choice over whether Company 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.

2.9. Respect data subject rights


Whenever Company 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 Company 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 (Data Subject Rights Policy) are followed.

3. Data Processor Principles

When Company processes Personal Data as a Data Processor, on behalf of a Customer which is the Data Controller, Company 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;

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	9 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		


- **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 Company 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 Company; 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 Company 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).

4. Data Security

Company 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;

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	10 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

- 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.

Company 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 Company becomes aware of a personal data breach, it must follow the procedures set out in the [InfoSec Be Secure Guide](#).

5. Sharing Personal Data with Third Parties

5.1. Sharing data with Data Processors and Sub-Processors

Company 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.

Company 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 Company to process Personal Data for which a Customer is the Data Controller, then the additional provisions set out at Section 3 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.


5.2. Sharing Personal Data with Data Controllers

Company 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 2 above, including being able to justify the sharing as set out at sections 2.1 and 2.2 above.

5.3. 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

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	11 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

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 Company 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.

5.4. 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.

6. Records of processing

Company 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), Company 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 Company, details of any transfers of Personal Data outside the European Union and a general description of the security measures in place, and:
 - ✓ where Company 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 Company 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.


7. Data Privacy Organisation

Company must appoint a data protection officer if this is required by the GDPR or if this is required by an applicable national law.

7.1. 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;

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	12 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

- 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.

7.2. 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 1; and
- report major privacy issues to the Group Data Protection Officer.

7.3. 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.

8. 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.

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	13 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

9. Monitoring Compliance

Company 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 Company 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. Company shall take adequate steps to remedy breaches of this Privacy Policy identified during monitoring or auditing of compliance.

Company 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.

10. Video Surveillance Policy

The Company implements automated processing of personal data through video surveillance systems at Company's sites to ensure the security of its buildings, property, staff and visitors.

Company's Video Surveillance Policy is provided in Appendix 4 (Company's Video Surveillance Policy).

Company's video surveillance policy, describes scope, objectives, operation and the safeguards adopted to protect personal data, the right to privacy and the other fundamental rights and legitimate interests of individuals processed by the Company's video surveillance system.

11. Data Privacy Guidance


If you have any data privacy questions or issues including the enforcement of the rights of individuals, please refer to the Practical [Data Privacy Guidance document](#).

The Company provides support with any data privacy related questions, comments, concerns or complaints or in case you wish to exercise any of your data privacy related rights through its country of group data privacy organization to be contacted at:

For country specific questions, please contact your [ABB Bulgaria Country Privacy Lead \(CPL\)](#).

For Function specific questions, please contact the dedicated [GDPR Function Leads](#).

Link to Bulgarian [Data Protection Commission \(www.cpdp.bg\)](http://www.cpdp.bg).

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	14 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

VII. ENCLOSURES

I. Appendix 1


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, Company must consult with the Competent Supervisory Authority in conjunction with the Global Data Privacy Officer.


	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	15 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

II. Appendix 2

1. Third Party Personal Data Transfer Policy

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

Nature of processing to be described	<ul style="list-style-type: none"> ✓ 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	<ul style="list-style-type: none"> ✓ Data Processor may only process personal data on clear, documented instructions
Data transfer	<ul style="list-style-type: none"> ✓ 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 ○ 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	<ul style="list-style-type: none"> ✓ All personnel authorised to process the personal data to be bound by confidentiality obligations
Security	<ul style="list-style-type: none"> ✓ Description of the technical and organisational measures to protect personal data
Sub-processing	<ul style="list-style-type: none"> ✓ Authorisation required to appoint sub-processors ○ 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	<ul style="list-style-type: none"> ✓ 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	<ul style="list-style-type: none"> ✓ 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

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	16 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		


Data Privacy Impact Assessments (DPIAs)	✓ Assist the Data Controller in conducting 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	<ul style="list-style-type: none"> ✓ 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 ○ Exception possible if retention required by applicable law
General assistance	<ul style="list-style-type: none"> ✓ 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	<ul style="list-style-type: none"> ✓ 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	<ul style="list-style-type: none"> ✓ 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

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	17 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

Data transfer	<ul style="list-style-type: none"> ✓ 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 ○ 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	<ul style="list-style-type: none"> ✓ All staff authorised to process the personal data to be bound by confidentiality obligations
Security	<ul style="list-style-type: none"> ✓ Description of the technical and organisational measures to protect personal data ✓ May be provided via link
Sub-processing	<ul style="list-style-type: none"> ✓ Customer authorisation required to appoint sub-processors, whether part of ABB or external ○ 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: <ul style="list-style-type: none"> ○ Relevant to the processing by the Sub-processor in the services agreement with the Customer ○ 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) ○ Duty to assist the Customer (Privacy Policy, section 3) ✓ Liability for acts of the Sub-processor
Data Subject rights	<ul style="list-style-type: none"> ✓ Assist the Customer in responding to these – so far as is possible and taking into account the nature of the processing
Personal data breaches	<ul style="list-style-type: none"> ✓ 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

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	18 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

	<ul style="list-style-type: none"> ✓ Report personal data breaches to the Customer without undue delay
DPIAs	<ul style="list-style-type: none"> ✓ Assist the Customer in conducting 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	<ul style="list-style-type: none"> ✓ Return or delete personal data at the end of the services, at the Customer's choice, and delete all copies of the personal data ○ Exception possible if retention required by European Law
General assistance	<ul style="list-style-type: none"> ✓ 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	<ul style="list-style-type: none"> ✓ Allow and contribute to audits, including on-site inspections, conducted by the Customer or an auditor nominated by Customer ○ Those auditing must follow the Audit Conditions

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	19 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

III. Appendix 3

1. Data Subject Rights Policy

Rights of Data Subjects

Whenever Company 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 Company 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 Company 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

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	20 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

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.

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	21 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

IV. Appendix 4

1. Company Video Surveillance Policy

1. Introduction

Video surveillance recording represents automated processing of personal data within the meaning of GDPR.

The Company employs video surveillance system at its sites and buildings on the territory of Bulgaria to ensure the security of its buildings, property, staff and visitors in the following sites:

- **ABB Bulgaria EOOD - Headquarters** - Sofia 1408; 89B, Vitosha Blvd., Millennium center, Building A, fl. 17
- **ABB Bulgaria EOOD - Turbocharger service station** - 9009 Varna; Odessos Shiprepair Yard, Island Zone
- **ABB Bulgaria EOOD - R&D Center** – Sofia 1330, Business Center Serdika, 2E, Ivan Evstratiev Geshov Blvd., Building 2, fl. 2, office 202
- **ABB Bulgaria EOOD - Branch Rakovski** – Industrial zone Rakovski, 4142 Stryama, 14 and 18, Industrial Road 1
- **ABB Bulgaria EOOD - Branch Sevlievo** – 5400 Sevlievo, 32 Nikola Petkov Str.
- **ABB Bulgaria EOOD - Branch Petrich** - 2850 Petrich; 1, Varna Str.

This video surveillance policy describes the video surveillance system at the above-mentioned sites and the safeguards adopted by the Company to protect personal data, the right to privacy and the other fundamental rights and legitimate interests of individuals filmed by the system's cameras.

2. Objective and Scope of the video surveillance system


The video surveillance system for which Company is responsible is one of the resources underpinning its mission of protecting its staff, property and information. It is therefore intended to carry out typical security tasks, including in particular control of access to buildings and to certain restricted access areas within these buildings. Use of the cameras is designed to prevent, detect and then document any security incident that occurs in buildings occupied by the Company or in the surrounding area, if this comes under its responsibility (forecourt, car park, garage, manufacturing and administrative premises). The term 'security incident' refers in particular to wrongdoing in the form of intrusion, theft, unauthorised access, break-ins, vandalism, assault, threats, and arson.

3. Operation

The cameras store all movements in the areas that they monitor, 24 hours a day and 7 days a week, unless otherwise indicated.

4. Systematic operational exclusions

The video surveillance system is under no circumstances used to monitor the legitimate activities of staff, service providers or visitors, checks on the quality of work and productivity levels.

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	22 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

Similarly, the video surveillance system is not used, even incidentally, to capture or process images in special data categories, such as race, ethnic origin, religious, political or trade union beliefs, and data relating to the health or sexual preferences of individuals.

Places in which individuals clearly consider that their privacy must be protected more strictly, such as bathrooms, changing rooms or other relaxation areas, cannot be equipped with a video surveillance system.

No webcams for public dissemination of video surveillance footage will be used in the areas covered by this policy.

5. Systems not covered by this policy

Video-intercom entry systems, video conference systems, and recording of images for documentary purposes at events such as conferences or training courses are not covered by this text.

6. Installation of video surveillance systems within Company premises

6.1. Analysis prior to installation

If it is planned to install a video surveillance system in a building or site occupied by the Company, the latter conducts a prior analysis to assess whether use of such equipment is appropriate and proportional to the purpose envisaged, in terms of the number of cameras, their location and the configuration of the system.

The operating schedule and recording arrangements of each system are established in accordance with the same criteria of necessity and proportionality. The same applies to definition of the quality of the camera footage, and therefore to the type of camera selected.

The purpose of this analysis is to reduce the risk of infringing the fundamental rights of any person, particularly with regard to personal data protection and privacy.

6.2. Building/Premise file


A file is created for each building or premise equipped with video surveillance. This file lists the type and number of active cameras /recorders in the building. Each camera is referenced by name and location.

6.3. Special cases of temporary video surveillance systems

Some investigations or monitoring relating to matters that are significant in terms of the issue at stake, the value of the damage involved or the risk posed to staff may require the temporary use of discreet and/or intentionally concealed video surveillance systems, which obtain footage of people who are not clearly informed of the surveillance. These systems will be used only when it proves to be impossible to obtain objective evidence by other means to identify the perpetrator(s) of disciplinary or criminal offences (for example, in cases of repeated bodily injuries, health and safety violations, thefts in the same place, arson, or repeated acts of vandalism, personal assaults, etc.).

Company keeps a register of the sites and usage periods involved, as well as the file reference for the relevant investigation.

In each case, Company obtains prior authorisation from the Country Managing Director and Country Privacy Lead.

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	23 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

7. Installation of cameras

7.1. Field of vision

7.1.1. Outside buildings

The installation of cameras outside the premises under the Company's responsibility is conditional on the identification of specific risks such as pedestrian health and safety, Company's asset protection, etc. and to take account of the obligations deriving from the security agreements of the Company. Camera's field of vision shall not include private spaces.

Outside courts belonging to Company buildings may be filmed in compliance with the principles of this policy. Outside courts belonging to Company buildings may be filmed in compliance with the principles of this policy.

7.1.2. Inside buildings

The purpose of installing cameras inside buildings is not to monitor the legitimate work of staff or to collect private data. As far as possible, the cameras' field of vision excludes the areas of usual activity of the staff, unless specifically required under the technological process and or safety reasons, subject to special cases of temporary video surveillance systems as described above.

Cameras are placed mainly at the entrances and exits of buildings or parts of buildings (entrance halls, vehicle access points, emergency exits, walls or fences surrounding the area under the Company's responsibility, sites accessible to the public outside), at entrances to restricted areas such as those containing valuable equipment or classified information, and internal areas in buildings, where access rights are differentiated with a view to monitoring by automated access systems.

The goal is to monitor the areas in which incidents jeopardising the security of the Company's staff, property and information are likely to occur.

7.2. Number of cameras

During the survey prior to installation of a video surveillance system, the number of cameras is examined in order to install as few as possible to achieve the legitimate goal in view.


7.3. Technical specifications of cameras and recording systems

The type of camera is chosen according to the degree of precision required for the goal in view. Most of the cameras used are fixed cameras. The video surveillance systems are not interconnected with other systems, with the possible exception of a recognition system for vehicle number-plates and drivers entering the garages of buildings occupied by the Company.

8. Viewing images

8.1. Live viewing – viewing images recorded less than 24 hours beforehand

Security officers at the entrance to the building can provide live viewing of images to enable immediate monitoring. The screen showing these images is placed in such a way as not to be visible to unauthorised third parties passing nearby. Images may also be viewed remotely, in a control room accessible to staff on duty. In certain cases, staff on duty may also view footage up to 24 hours old, so that they can react to any dangerous situation or infringement.

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	24 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

Life viewing can be also introduced in case technological process requires so for identified risks, such as health and safety of operators of high risk equipment or non-stopping manufacturing processes.

8.2. Deferred viewing (images recorded more than 24 hours beforehand)

When the technical equipment allows it, the images filmed may be viewed by authorised officials if justified by a security incident, such as an alarm being set off or a security anomaly being detected (e.g. a door of a building found open, recent live viewing of an incident, a witness reporting an incident), or as part of an inquiry procedure for duly referenced cases.

8.3. Maintenance staff

The maintenance staff responsible for technical maintenance of the systems have access to all the system components, including recordings, but may not copy images onto any media whatsoever, download them onto independent devices, or transmit them electronically.

8.4. Requests to view images from an individual concerned

An individual, member of staff, service provider, visitor or passer-by who entered into the field of one or more cameras at any time may exercise their right to view the images directly concerning them, and to correct and complete personal data concerning them. However, this right must be strictly limited by the protection of the personal data of third parties who also appear in these images. Therefore, if it is not possible to isolate the images in which the requester alone appears, using standard means and without a disproportionate investment with regard to the importance of the images sought, the individual concerned is informed of the technical reasons making it impossible to provide the images.

Corrections can only be made by erasing the images in question. This may be done following any legitimate request to erase images that do not constitute objective evidence in the event of an offence, unless there are unforeseen technical obstacles.

A response is given as quickly as possible, and as far as possible within 30 days for any consultation requests. In technically complex cases, unless there are preventing factors as described above, the access authorisation is issued within 90 days of the request being received.

The Company reserves the right to seek reimbursement of the costs incurred in fulfilling the request from the requester(s), if the amount is kept within reasonable proportions.

8.5. Copying and transferring images to third parties


Company only sends copies of the images it holds to duly authorised administrative or judicial authorities in the framework of investigation cases. The request must be made in writing and precisely delimit the period and the nature of the images requested. An assessment of how necessary the transfer is and whether it is compatible with this policy is carried out to this end.

Aside from the competent judicial authorities, the Local Disciplinary Committee (LDC), within the meaning of Country Internal Control Over Integrity Instruction, may obtain such data.

9. Recording images

9.1. Place of recording

Images can be recorded either locally in the building equipped with the cameras, or centrally in a technical area in another Company building. Recording systems are subject to physical and

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	25 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

electronic protection, such that no unauthorised person can view, print or copy the images in any way.

9.2. Access to the systems

Only equipment operating and maintenance staff and those in charge of investigations on ad hoc basis may access the relevant equipment.

Any failing that may allow or that may have allowed unauthorised access to the data recorded must be notified without delay in writing to the Company Country Managing Director and the Country Privacy Lead.

9.3. Transmitting images for remote viewing

The persons referred to in point 9.2 above may connect to the system remotely, provided that this is technically possible and that the data is transmitted in a secure manner.

9.4. Length of time for which recorded images are held

Recordings will not be kept beyond the period necessary for achieving the objective of the video surveillance system. Experience shows that requests from judicial authorities and/or the police for access to and/or copies of images as part of an inquiry launched after an offence has been committed generally take a certain amount of time, due to the strict application of the procedures. It is therefore reasonable to set the time limit for holding recorded images at 30 days.

The systems must be programmed to erase images automatically after this 30-day period. If it is impossible to do this automatically, manual erasing of the footage must be scheduled.

9.5. Removal of decommissioned, obsolete or broken equipment

All equipment or components that contain or have contained video surveillance footage must have all data definitively and irreversibly removed using the safest and most recent techniques, before being decommissioned, removed or designated for destruction so that the data cannot be reconstructed and unduly used.

10. Publicity


10.1. Posters

Each entrance (entrance halls, vehicle access points) to buildings equipped with cameras and/or recording systems for the images obtained by the cameras is provided with a poster (sticker, plate) bearing the symbol for a camera.

11. Staff training and confidentiality clauses

Any official who has access to video surveillance footage or who has been authorised to carry out work on such images must sign a confidentiality declaration and attend training on personal data protection.

Similarly, staff members of firms supplying security services or maintenance services for video surveillance installations within buildings occupied by the Company, who are likely to see video surveillance footage, sign a confidentiality declaration and attend training on this subject organised by their firms.

	ABB BULGARIA EOOD	Code:	CI/LI
	COUNTRY INSTRUCTION	No.:	01
		Date:	25.05.2018
		Page:	26 of 26
Process Owner:	Country Privacy Lead		
Concerning:	Company Privacy Policy		
Replacing:	<i>No previous document</i>		

12. Implementation

The provisions of this policy will be updated periodically.

At the same time, the existing systems are being analysed in order to ensure their compliance with this policy.

13. Contact point

For any questions or for information on the policy outlined in this document, please contact the Country Privacy Lead.

V. REVISION HISTORY

Previous Version <i>(ID and date)</i>	New Version <i>(ID and date)</i>	Approved by	Revision Notes
n/a	CI/LI 01-25.05.2018	CMD, CCFO	<i>n/a</i>

VI. FINAL PROVISIONS

This instruction shall come into effect as from the date of being announced.

Not knowing the provisions of this Instruction will not be accepted as an excuse for not applying it. Not observing the provisions of this Instruction will be treated as a breach and administrative sanctions and penalties will be applied, in accordance with the Internal Regulations of ABB in Bulgaria, Labour Code and other applicable Legislation.

This instruction is an internal regulation of the Company and will be modified from time to time.

ABB BULGARIA EOOD		
Approval steps	Names and title	Type of the approval/ signature
<i>Approved by:</i>	1. Marcel van der Hoek - CMD 2. Maurizio Riva - CCFO	Digitally/ WF
<i>Verified by:</i>	1. Jeny Marekova - CPL	Digitally/ WF
<i>Issued by:</i>	1. Tomislav Velichkov - CIMSM	Digitally/ WF