Bosch Access Control Systems
General Data Protection Regulation (GDPR)

1 Introduction

The GDPR has been in force since the 25th of May 2018. As a regulation it is directly applicable to all EU member states without the need for national implementing legislation. As information processed and stored by Bosch access control systems is classified as "sensitive", the GDPR impacts these systems, too. This document provides insights into the new legislation and describes how Bosch access control systems can be designed and configured to help organizations to comply with this new regulation.

Disclaimer

The contents of this description of the GDPR are non-binding but as accurate as possible. Furthermore, the present document focuses on Bosch access control systems only. Further measures for GDPR compliance, than those mentioned within this document, may be undertaken depending on the type and scope of the business and software used. GDPR compliance cannot be reached with the adjustment of an IT system alone: The processing activities have to be in compliance to the requirements. These are not considered in this document.

1.1 Content

Section 1 will describe the functional requirements as they were extracted from the GDPR by the Bosch legal teams. Section 2 will describe how these functional requirements affect the system design phase of a project. Section 3 will describe how these functional requirements affect the system installation and configuration phase of a project. Last, but not least, a list with frequently asked questions and a dictionary are included. The present document references to “Bosch Access Control Systems” which belongs to Business Unit Access Control & Intrusion Systems. Concretely, the three products “Building Integration System (BIS)”, “Access Management System (AMS)” and “Access Professional Edition (APE)” are meant implicitly. Details on e.g. configuration aspects are provided as part of the product´s documentation material.

1.2 General Data Protection Regulation (GDPR)

1.2.1 Summary

"*After four years of preparation and debate the GDPR was **finally approved** by the EU Parliament on **14 April 2016**. It will enter in force 20 days after its publication in the EU Official Journal and will be directly apply to all member states two years after this date. Enforcement date: **25 May 2018** - at which time those organizations in non-compliance will face heavy fines.*

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy."

Source: https://www.gdpreu.org/

The full text of the "*Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*" can be found on the website of the European Union.

1.2.2 Key concepts

A description of the key concepts can be found on https://www.gdpreu.org/the-regulation/key-concepts/.

Warning

The GDPR will not only affect installations within the border of the EU. The territorial scope of the GDPR has increased relative to its predecessor.

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
    1. (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
    2. (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Source: https://www.gdpreu.org/the-regulation/who-must-comply/

2 Requirements

2.1 Functional Requirements

Bosch has analysed the GDPR. The analysis resulted in the functional requirements listed in the table below. These functional requirements are applicable to all systems that process personal information and not specific for an access control system. The third column describes how the requirement is related to a Bosch access control system.

ID	Feature / Topic	Description
1- 6, 18	Consent	The first six requirements are related to consent: a data subject needs to agree with the processing of his or her personal data by "signing" a declaration of consent.
7	Implement a compliant data protection notice in respective language.	Data subjects must be informed (a) how to proceed to rectify/delete personal data, (b) how to withdraw a consent, (c) how long personal data is stored (d) if personal data is transferred to a third country or to an international organization, and the appropriate safeguards pursuant to Article 46 relating to the transfer and (e) on which legal basis personal data is processed.
8	Make a data protection notice available to data subjects in an easily accessible way.	The operator of the access control system must make the data protection notice available to data subjects in an easily accessible way.
9	Ensure data protection notice versions are stored with a time-stamp.	As a system operator you are obliged to prove that you have provided the mandatory information to data subjects by making the data protection notice available.
10	Ensure a time-stamp is stored when the personal data is collected.	Whenever personal data is collected, the application must ensure the time-stamp is stored together with the data collected and is available for reporting.
11	Ability to provide detailed information about personal data processed to the data subject.	The controller is obliged to provide access to and information on the personal data processed to a data subject (including a copy of the personal data).

12	Ability to rectify personal data and ensure information of recipients of such rectification.	The controller is obliged to rectify personal data upon a data subject's request and to inform all recipients of such personal data in order to ensure that personal data is kept correct and updated.
13	Enable data subject to erase its personal data.	If the purpose of the data processing allows it, the application can provide a feature in the user interface to the data subject to delete his data on his own request.
14	Ability to erase personal data and to ensure information of recipients of such erasure.	If personal data concerning a specific data subject is to be erased by the controller, the application must provide the means to permanently delete or anonymize the respective personal data on all storage locations known
15	Support automatic erasure / anonymization of all personal data after all valid purposes are fulfilled.	The controller is able to define cases in which personal data can be automatically erased subject to certain conditions (for example after all legally valid purposes are fulfilled and no retention periods apply), so that personal data is never stored/processed without a valid legal basis purpose.
16	Ability to restrict / unrestrict processing of personal data.	If the controller wants to restrict the processing of personal data, the application must mark the data related to the data subject as restricted, and prevent the further processing of the data with exception of data storage.
17	Ability to export certain personal data provided by the data subject in a machine-readable format.	The controller is obliged to be able to transmit certain personal data provided by the data subject upon such data subject's request in a structured, commonly used and machine-readable format either to the data subject or to another controller, to facilitate the change between service providers.
19	Default Settings for the processing of personal data must be limited to the processing necessary for the specific purpose.	The controller is obliged to only use default settings that limit the processing of personal data to the extent necessary for the specific purpose.

2.2 Concepts

ID	Topic	Description
20	Data quality	Personal data should be relevant to the purposes for which they are used, and should be accurate, complete and kept up-to-date.
21	Purpose specification	The purposes for which personal data are collected should be specified and any subsequent use must be limited to that specification.
22	Use limitation	Data should not be disclosed, made available or otherwise used for purposes other than those specified except a) with the consent of the individual or b) by the authority of law.
23	Security safeguards	Data should be protected by reasonable security safeguards to protect against loss, destruction, use, modification or disclosure.

24	Openness	There should be a general policy about openness with respect to personal data.
25	Individual participation	An individual should have the right to find out information about their data and to have incorrect data erased or rectified.
26	Accountability	A data controller is accountable for complying with these measures.

3 System Design

Next to the requirements of the system itself, article 35 requires an organization to conduct a data protection impact assessment.

"*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*"

Source: GDPR full text, Article 35, section 1 (page 164)

3.1 Access Control Readers

Related to requirement(s): [20, 21]

Access control readers should only be installed in areas where they serve a specific goal, e.g. securing facilities or objects. The installed location of a reader, which gathers personal data in case a badge is presented to gain access, should be justified.

3.2 System resilience

Related to requirement(s): [23]

Hardware mechanisms (e.g. redundant components) as well as software mechanisms (e.g. SQL server backup) are available to minimize the chance data is lost.
Hardware mechanisms (access control to rooms, physical locks, and others) as well as software mechanisms (encryption of data, the architecture of the software itself) are available to minimize the chance data is stolen.

Note:
It is highly recommended to always use the latest Bosch access control software which provides the latest IT security updates.

4 System configuration and operation

4.1 Consent

Related to requirement(s): [1-8, 18]

Each and every user (cardholder) of an access control system needs to be enrolled to the access control system first. In order to get a badge which is used to get access to parts of a facility by presenting the credentials to the reader, the receiver of the badge should sign a confirmation. A personalized acknowledgement can be generated by the access control systems, too. [related to requirements 1-6, 18]

The confirmation should include the receipt of the badge and information on data processing and storage within the access control system. Having this, the cardholder explicitly gets notification and needs to actively agree. [related to requirements 7, 8]

4.2 Time-service

Related to requirement(s): [10]

Offering a reliable time-service to entire access control environment ensures that all the components, such as hardware and software clients, are using the same, synchronized clock. Bosch can provide, on request, a recommendation on how to set-up a reliable time-service within the access control system.

4.3 Personal data overview

Related to requirement(s): [11]

The Bosch access control systems offer the possibility to print reports that contain all stored personal data. As these reports can be printed, too, the subject (cardholder) may get a copy of it.

4.4 Access control user interface

Related to requirement(s): [12, 20, 23]

The user interfaces of the Bosch access control systems allow to edit personal data if the corresponding authorizations are available (e.g. by an administrator or operator). Changes can be tracked, displayed and printed, too.

4.5 Removing personal data

Related to requirement(s): [13, 14, 15, 25]

If the controller (e.g. operator) has the required authorizations, all personal data can be deleted for a selected person. Access events can be deleted for the overall access events in a specified time period.

4.6 Restrict event log and personal data

Related to requirement(s): [16]

Access to event logs and personal data can be restricted to specific (groups of) operators.

4.7 Export

Related to requirement(s): [17]

Personal data and event logs can be exported in several file formats.

4.8 User authorizations

Related to requirement(s): [19, 22, 23]

The system allows complex user rights configurations. This allows a system administrator to give access to specific system components and system functionality to specific operator (groups). Additionally, most operator tasks are logged in the system logbook for further reviews.

5 Conclusion

After intensive discussions with experts on all of these topics, Bosch has concluded that the current Bosch access control products (including Bosch access controllers and software) will allow an organization to be GDPR "compliant".

6 Frequently Asked Questions

The questions and answers below are gathered from several sources for the readers' convenience. At the moment of writing this document the answers are valid.

Question	Answer	Source
Who does the GDPR affect?	"The GDPR not only applies to organisations located within the EU but it will also apply to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location."	https://www.gdpreu.org/
Does my business need to appoint a Data Protection Officer (DPO)?	"DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data (Art. 37). If your organization doesn't fall into one of these categories, then you do not need to appoint a DPO."	https://www.gdpreu.org/
What is considered as "sensitive personal data"?	"Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, ..."	GDPR full text, Article 4
Are images captured by a video surveillance system considered sensitive?	Yes, as a photo can reveal racial or ethnic origin this information is considered sensitive.	GDPR full text, Article 4

7 Dictionary

This section provides some important definitions of terms. The source of these definitions, and all other definitions, can be found in: GDPR full text Article 4, page 112.

Term	Definition
Controller	"The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;"
Data subject	"...identified or identifiable natural person..."
Personal data	"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"
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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"
Pseudonymisation	"...means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;"