BOSCH
Invented for life

BVMS - GDPR

Author: Verhaeg Mario (BT-SC/PAS4-MKP)
Date: 26 August, 2019

1 Document information

Disclaimer
The contents of this description of the General Data Protection Regulation (GDPR) are non-binding and might be outdated. Bosch recommends to seek legal advice for every video surveillance installation deployed within the European Union. 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.

Project	General Data Protection Regulation
Reference	http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf
Version	32
Last modified	26 August 2019

1.1 Version history

Version	Date	Author	Comment
32	2019-26-08	Verhaeg Mario (BT-SC/PAS4-MKP)	

2 Introduction

The GDPR is enforced on 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 captured, processed and stored by video surveillance systems is classified as "sensitive" the GDPR will cause significant impact on the video surveillance installations throughout Europe. This document gives insights into the new legislation and describes how a video surveillance system can be designed and configured in order to help an organization comply with this new regulation.

Disclaimer
The contents of this description of the General Data Protection Regulation (GDPR) are non-binding and might be outdated. Since the publication of this guide the European Data Protection Board (EDPB) has issued a paper specifically targeted at video surveillance installations: GDPR video surveillance guide
Bosch recommends to seek legal advice for every video surveillance installation deployed within the European Union. 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.

Person identification
As of BVMS 10.0 person identification technology can be used, which generates biometric data. The processing of biometric data is, in general, not allowed. Exceptions are described in article 9 section 2.

2.1 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 phase of a project. **Section 4** lists some general exceptions which are applicable for all video surveillance systems. Last, but not least, a list with frequently asked questions and a dictionary is included.

2.2 General Data Protection Regulation (GDPR)

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 application in all members 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: http://www.eugdpr.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.

2.2.1 Key changes

A description of the key changes can be found on http://www.eugdpr.org/key-changes.html.

Warning
The GDPR will not only affect installations within the border of the EU.
"*Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR,* ***as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location.***"
Source: http://www.eugdpr.org/key-changes.html

2.3 Information

Website	Description
http://www.eugdpr.org/	This website is a resource to educate the public about the main elements of the General Data Protection Regulation (GDPR)
EU data protection rules	Official EU website. Stronger rules on data protection mean people have more control over their personal data and businesses benefit from a level playing field.
Wikipedia	General Data Protection Regulation on Wikipedia.
http://www.cloudview.co	Whitepaper on GDPR.
https://edpb.europa.eu/	The EuropeanData Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities.

3 Requirements

3.1 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 a video management system. The "Description" column describes how the requirement is related to a video surveillance system.

ID	Description	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. This is not applicable for video surveillance systems, as it would not be possible to ask all data subjects to signed such a declaration of consent before they enter a premise.
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 video surveillance 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

ID	Description	Description
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.

3.2 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.

4 System design

4.1 Data protection impact assesment

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)

4.2 Camera positioning

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

Video cameras should only be installed in areas where they serve a specific goal. The installed location of a camera, which is gathered personal data (or biometric data), should be justified.

4.3 System resilience

Related to requirement(s): [23]

Hardware mechanisms (RAID, redundant components) as well as software mechanisms (for example dual recording) 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.

5 System configuration and operation

5.1 Signage

Related to requirement(s): [7,8]

The data protection notice cannot be made easily available to data subjects in the context of a video surveillance system.

Signage
Existing legislation already enforced the usage of signage which informs the audience they, and their properties, are monitored by a video surveillance system.

1. *"Signage should be clearly **visible** and **readable**. It will also need to show details of the organization operating the system, the purpose of its use and who to contact if there are any queries.*
2. *Signs should be an appropriate size in relation to its context. If the sign needs to be seen by a car driver it should be bigger, and if it is in a shop then a small sign would be more suitable.*
3. *All staff should know what to do and who to contact if a member of the public asks about the CCTV system. Any signs in a public area must show the organization or authority responsible for the systems.*
4. *Take care when it comes to positioning your CCTV cameras. Although your cameras may be positioned on site, they may still capture images of people walking by. If this is the case your CCTV signage should be visible outside the business too.*
5. *Depending on the location, **new signage alone** – without CCTV – might be a sufficient and cost-effective deterrent to thieves. A movement-activated lighting system in somewhere like a car park could serve a similar function while consuming less electricity."*

Source: IFSEC Global

5.2 Time-service

Related to requirement(s): [10]

Offering a reliable time-service to entire video surveillance environment ensures that all the components, such as cameras and software clients, are using the same, synchronized, clock. Bosch provides a recommendation on how to set-up a reliable time-service within the video surveillance environment. This recommendation is available on the Bosch Building Technologies community: BVMS - Configure Time services.

5.3 Video Authentication

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

The video authentication functionality should be enabled. This allows system operators to check (either during export or on the actual recorded video) if (unauthorized) modifications are made to the recorded video footage.

5.4 Removing personal data

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

A self management erasure functionality may be considered **only** if personal data can be erased **without further assessment** (for example, regarding retention obligations under applicable tax or commercial law). Summarized: it would not be allowed for people which appear on recorded footage to delete this footage themselves. The system includes a retention time mechanism which automatically removes recorded footage and logbook data after the maximum retention time has passed.

5.5 Removing biometric data

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

A self management erasure functionality may be considered **only** if personal data can be erased **without further assessment** (for example, regarding retention obligations under applicable tax or commercial law). Summarized: it would not be allowed for people to delete their own biometric data from the system. The system includes a retention time mechanism which automatically removes biometric data from the logbook as well as a mechanism to remove biometric data manually by anonymizing information in the logbook and removing subjects from the person identification subject list.

5.6 Restrict access to data

Related to requirement(s): [16]

Access to person and biometric data (recorded video and logbook) can be restricted to specific (groups of) operators.

5.7 Video Export

Related to requirement(s): [17]

Video footage can be exported in several file formats, proprietary (Bosch) as well as open standards (mov, asf). The proprietary export format can be read by Bosch software, the open standard exports can be read by industry standard software (Apple Quicktime, VLC, Windows Media Player, etc...)

5.8 Export biometric data

Related to requirement(s): [17]

Biometric data can be exported using the logbook export functionality for operators(groups) who are authorized to do this.

5.9 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 (cameras, sensors, maps) and system functionality (live, recording, alarms, export) to specific operator (groups). Additionally most operator tasks are logged in the system logbook for further reviews

5.10 System protection

Related to requirement(s): [23]

Bosch recommends implementing the tips mentioned in the data security guidebook to decrease the risk of personal or biometric data being accessed, modified, or destroyed by unauthorized persons.

6 Exceptions

6.1 Provide personal information

Related to requirement(s): [11]

At this moment the video surveillance system is not able to identify a person without adding a, separate, person identification system generating biometric data. Personal data can be (theoretically) provided, but would require the operator to manually browse thousands of hours of recorded video.

Exception
"*The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22,* ***unless the controller demonstrates that it is not in a position to identify the data subject.***"
Source: GDPR full text, Article 12, section 2 (page 129)

Article 24
"*Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*" A specific definition of "*appropriate*" is not available.
Source: GDPR full text, Article 24 (page 150)
If, in the context of video surveillance, appropriate technical and organizational measures are not available, the requirement can be ignored. For example, at this moment it is fair to state that implementing a facial recognition system (which currently only works in limited use-cases) over hundreds of cameras is an unproportional request due to the related costs. Of course, once the costs of such a system go down, it might not be unproportional anymore in the (near)future.

7 Conclusion

After some intensive discussions with experts on all of these topics, Bosch has concluded that the current video surveillance products (including cameras, software and recording hardware) will allow an organization to be GDPR "compliant".

8 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.*"	http://www.eugdpr.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.*"	http://www.eugdpr.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
What is considered as "biometric data"?	"*Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;*"	GDPR full text, Article 4
Are images captured by a video surveillance system considered as sensitive personal data?	Yes, as a photo can reveal racial or ethnic origin this information is considered sensitive.	GDPR full text, Article 4

Question	Answer	Source
Does the GDPR require the system to anonymize all data subjects by using of "pixelization"?	Pixelization is a technique whereby any moving object appearing in front of a video surveillance camera is blurred. In the context of the GDPR this process is called pseudonymisation. In contrast to what is marketed by many, data subjects do not have to be anonymized and therefore the use of pixelization software is not required. However, "*Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent... the controller shall...take into account: the existence of appropriate safeguards, which may include encryption or pseudonymisation.*" Summarized and put into context: if the position of a camera cannot be justified, pseudonymisation may be used to keep a legal basis for the position of that specific camera.	GDPR full text, Article 6, section 4
How does GDPR influence the deployment of person identification?	According to article 9 the processing of biometric data is prohibited: "*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*"	GDPR full text, Article 9, section 1
Does GDPR allow processing of biometric data at all?	GDPR only allows processing biometric data based on the description of article 9 section 2, in which exceptions on article 9 section 1 are described.	GDPR full text, Article 9, section 2

9 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;*"