



**BOSCH**


Invented for life

## **BVMS Person Identification - Data Protection Information**

Author: Verhaeg Mario (BT-SC/PAS4-MKP)  
Date: 19 September, 2019

<b>1 Document Information</b>	<b>3</b>
1.1 Version History	3
<b>2 Introduction</b>	<b>4</b>
2.1 Importance of GDPR	4
2.2 Data Privacy and Protection at Bosch	4
2.3 How Does Person Identification Work?	4
<b>3 Legal Framework</b>	<b>5</b>
<b>4 Processing of Personal Data and Special Categories of Personal Data</b>	<b>6</b>
4.1 Video Surveillance System	6
4.2 Video Surveillance System with Person Identification	6
<b>5 System Architecture</b>	<b>8</b>
<b>6 Technical Measures</b>	<b>9</b>
6.1 Authorization and access rights management	9
6.2 Authentication	9
6.3 Pseudonymization and data erasure	10
6.4 Input control	10
6.5 Customer self-service	10
6.6 Encryption	10
6.7 Threshold Probability	10
<b>7 Recommendations for on-premise solutions</b>	<b>12</b>

# 1 Document Information

Project	BVMS
Reference	n/a
Version	50
Last modified	 19 September 2019

## 1.1 Version History

Version	Date	Author	Comment
50	2019-19-09	Verhaeg Mario (BT-SC/PAS4-MKP)	

## 2 Introduction

This document aims to provide concerned parties, such as customers, users, operators or consultants, with an overview of data privacy and protection related features of BVMS Person Identification. Moreover, this document describes how data, as processed during the Person Identification steps, can be classified. Finally, this document lists technical measures for data protection in the context of BVMS Person Identification.

### 2.1 Importance of GDPR

The General Data Protection Regulation 2016/679 (GDPR) on the protection of natural persons with regard to processing of personal data and on exchange of such data became effective on 25 May 2016 and is repealing existing EU Directive 95/46/EC. The GDPR regulates the processing (handling) of personal data in the European Union. The objective is to protect the fundamental rights and freedom of natural persons and in particular their right of protection of personal data. Personal data are all the information which relate to an identified or identifiable natural person, for example, names, addresses, telephone numbers or e-mail addresses which are or can be the expression of the identity of a person.

Special categories of personal data in the sense of GDPR are information about a person, which are especially protected by the GDPR and therefore the data processing is subject to strict conditions. Special categories of personal data are, for example, racial or ethnic origin, genetic data, health data or biometric data. Art. 4 GDPR contains definitions of these terms. Before processing any personal data the national legal framework (see 3 Legal Framework) must be examined.

We recommend to contact the responsible supervisory authorities in order to eliminate legal uncertainties.

Data Protection is relevant and there are high penalties and loss of reputation, if legal frameworks are not met.

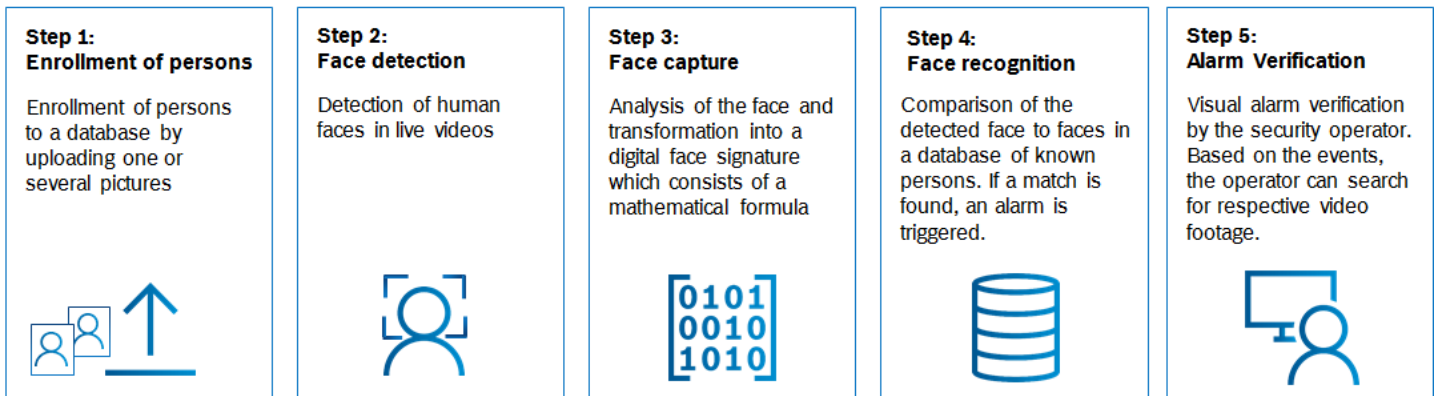
### 2.2 Data Privacy and Protection at Bosch

Worldwide, some 1,000 associates work for Bosch as data security officers and data security partners. They provide their colleagues with advice on matters of data protection and information security. In consequence, data protection and data security are firmly anchored in the development process for new products and services. We will not start marketing these until we have proven – e.g. by means of penetration tests – that our data protection and security measures are effective.

We assign our in-house data-protection and IT-security experts to development projects to make sure these aspects are given full consideration at all times.

### 2.3 How Does Person Identification Work?

- Person identification is the automated process of identifying a person by his / her face
- It detects, captures and analyzes facial patterns with the objective to find a match in a database of known persons
- If a match is detected and reported by the system, the security operator as human intelligence verifies the alarm



During the Person Identification steps, personal data (i.e. photo and video), including special categories of personal data (i.e. biometric data), are processed by the system.

## 3 Legal Framework

Legislation	Region	Summary
GDPR	European Union	<p>Using the video surveillance system requires a legal framework. The GDPR is the legal basis for processing of personal data in Europe. Examples for the legal framework for processing of personal data are Art. 6 (1) GDPR and Art. 9 (2) GDPR, if special categories of personal data are processing, e.g. biometric data.</p> <p>Guidelines published by official authorities and / or boards, such as the European Data Protection Board (EDPB) Guidelines 3/2019 on processing of personal data through video devices can be helpful to give an orientation for the evaluation.</p>
National regulations	European Union	<p>Use of a video surveillance system can be also regulated in national regulations (Art. 9 (4) GDPR).</p> <p>The relevant national regulations should be examined.</p>
National regulations	Non-European Union	<p>Use of a video surveillance system can be regulated in national regulations.</p> <p>The relevant national regulations should be examined.</p>

## 4 Processing of Personal Data and Special Categories of Personal Data

### 4.1 Video Surveillance System

A video surveillance system processes (including display as well as storage) a huge amount of data. However, such a system can at most automatically classify the *type* of an object (person, car, bike), but not classify the *identity* of that object.

This functionality allows, for example, an operator to search for "persons" or "cars", but does not allow him to search for person "John Doe" or for the car with license plate "M-12345".

As a result, most of the data processed by a traditional video surveillance system is classified as ("normal") **personal data** and listed in the table below.

Data type	Definition
Video Frame	Single frame out of a video stream.
Video Recordings	Video Stream.
Recording Time Camera	Timestamp (visible or invisible) which is stored in the video recordings.
Recording Location Camera	Location data which enable the correlation of camera id and its position.
Person Trajectory (Single Camera)	Data consisting of multiple location and time entries to describe movement patterns in a single camera`s field of vision.
Person Trajectory (Multiple Cameras)	Data consisting of multiple location and time entries to describe movement patterns combined over multiple cameras.
Event Log (Id. Events, DB Modifications)	Logbook in BVMS.

### 4.2 Video Surveillance System with Person Identification

New technologies enable the system to uniquely identify persons who are captured by the cameras connected to the video surveillance system.

Once the system is able to uniquely identify persons, some of the data is considered **Special Category of Personal Data** in the sense of GDPR.

This allows, for example, the operator to add the picture of "John Doe" to the system and have the system notify him when "John Doe" appears in front of one of the cameras.

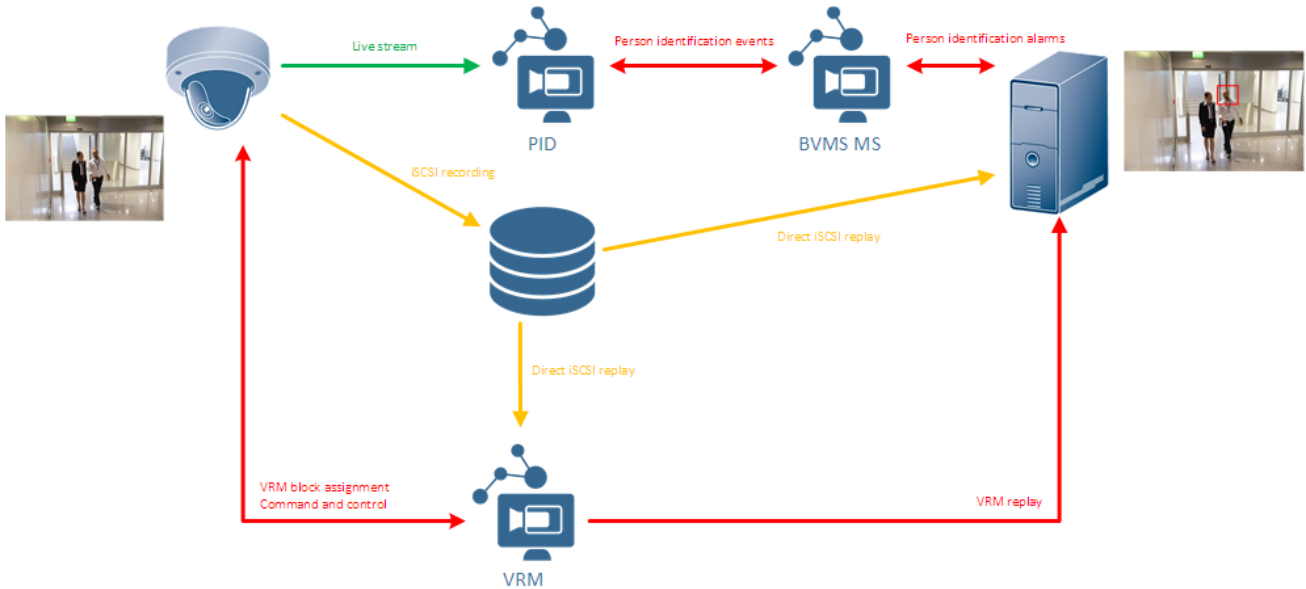
When extending BVMS with the Person Identification functionality, the data listed in the table below is processed in addition to the data listed above, which includes a special category of personal data in the sense of GDPR, i.e. biometric data.

Data type	Definition	Content	Classification
Passport Photo	Used as Input for "Facial Vector from Passport Photo". Also stored (raw) in "Subject Database".	Single Person	Personal Data
Name	Name in clear text for subject management in "Subject Database".	Single Person	Personal Data
Facial Vector from Passport Photo	Facial Vector generated from "Passport Photo" as input for the "Subject Database".	Single Person	Special Category of Personal Data

<b>Data type</b>	<b>Definition</b>	<b>Content</b>	<b>Classification</b>
Facial Vector from Video	Facial Vector generated from video data (multiple sources).	Single Person	Special Category of Personal Data
Subject-ID	Subject-ID generated for each new subject entry in the "Subject Database".	Single Person	Personal Data
Subject Database	Subject list with multiple entries of "Name", "Passport Photo", "Facial Vector from Passport Photo" and "Subject-ID", organized in groups.	Multiple Persons	Special Category of Personal Data
Identification Event	Successful identification of a facial vector. The event in the Log will contain: Time, (Camera)-Location, Subject-ID	Single Person	Personal Data

# 5 System Architecture

The video data and metadata (without person identification) is generated by the camera, and if recording of this data is enabled, is stored on an iSCSI drive. This video data can be replayed and the metadata generated by the camera can be searched for specific events. The video data itself, and the related metadata, is considered personal data. Additionally system events, actions and alarms are stored in the BVMS Logbook which is located on the BVMS MS (Management Server).



If the Person Identification functionality is enabled, the camera video data is also sent to the Person Identification Device (PID). The PID first attempts to find faces in the video. Once a face is detected, its facial features are determined and translated in a so-called face vector. A face vector is a unique mathematical representation of the face of a person. Every time this specific person appears in front of any camera, a face vector is generated. This allows the system to identify a specific person, even though this person is recognized in a different location under different circumstances (e.g. differing camera angles, varying light conditions, etc.). As the face vector can be used to uniquely identify a person, this is considered biometric data.

Based on this functionality, the security operator is able to instruct the system to search for a specific person. This is done by adding a photo of a person's face to the subject database. Managing the subject database is done from the BVMS Operator Client. Once a subject is added, the Operator Client sends the photo to the PID. Using the process described above, the PID searches for a single face in that photo, and generates a face vector. Both the photo and the face vector are stored in a subject database on the PID.

Once The PID has detected a face, it compares the face vector of the detected person in front of the camera with the face vectors stored in the subject database. If it finds a match between the two face vectors, it means that the system has detected a subject and an event is send to the BVMS Management Server. Depending on the configuration this event can be stored for later investigations. If the PID cannot find a match between the detected face vector and the subject database, the detected face vector is discarded and not stored within the PID.

Besides the PID specific description, data protection in general is explained in the document [BVMS - Securing the Security System](#).



## 6 Technical Measures

This section describes the technical measures that are available to manage both the personal and the special category of personal data in the sense of GDPR, i.e. biometric data. The technical measures outlined below follow a privacy by design approach.

Information related to general software security measures are described in the [BVMS - Securing the Security System](#) article.

### 6.1 Authorization and access rights management

BVMS has extensive authorization and access rights management. User groups (which can also be related to an enterprise user management environment) can be created, and can contain multiple users. For each user group, operating and configuration permissions can be set.

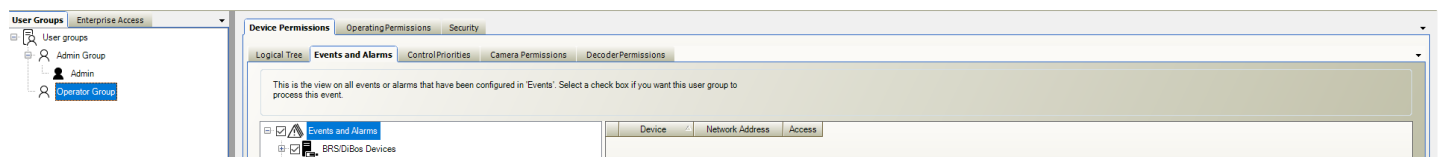
Following the privacy by design approach, the system contains, by default, two user groups: for the "Admin Group" all permissions are set, whereas for the "Operator Group" only the essential operator permissions are enabled. Access rights management itself (modifying who has access to the system and which functionality is permitted) is, by default, available for the "Admin Group", but can be (optionally) enabled for other user groups as well.

In order to ensure that alarms are not being missed by the operators, privacy by default approach was not followed. Instead emphasis was put on usability of the system and alarms were enabled for all operators to ensure that critical alarms were received.

The following functionality can be restricted by user group:

- PTZ control of dome cameras
- Allegiant trunk lines
- Print and save; Alarm display
- Playback; Logbook access
- Operator event buttons
- Close operator client
- Minimize operator client
- Audio Intercom
- Manual alarm recording
- Set reference image
- Change password
- Arm intrusion panel
- Force arm intrusion panel areas
- Disarm intrusion panel areas
- Bypass intrusion panel points
- Unlock intrusion panel doors
- Secure and unsecure intrusion panel doors
- cycle intrusion panel doors
- Person management.

The login can be restricted with a login schedule, the access to specific devices can be enabled or disabled and the event subscription can be tailored.



### 6.2 Authentication

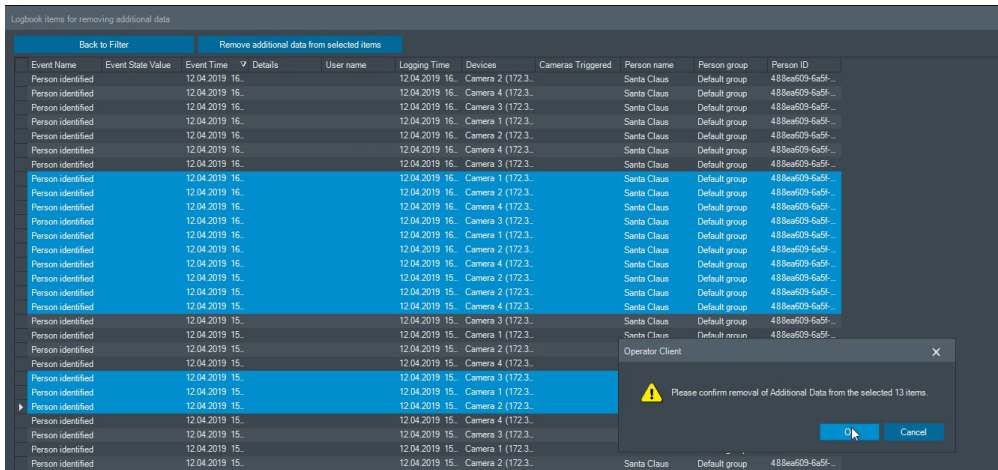
The users of the system are authenticated based on their user name and password. The system contains account policies which allow the system administrator to enforce the usage of strong passwords, including a minimum password

length, and a maximum password age. To further decrease the risk of misusing data a four-eye principle can be applied on the login process (dual authorization). This means that two users need to authenticate themselves for login before the system enables them to access the defined system's functionality.

### 6.3 Pseudonymization and data erasure

For each event that is triggered by the system it is possible to configure whether the event is transformed into an alarm (notifying the operator of the event) and whether the related event data is stored into the BVMS Logbook. For each camera managed by the system, the recording parameters (including the minimum and maximum retention time) can be configured as described in the [BVMS - Policy Based Recording](#) article.

The biometric data stored in the BVMS logbook as well as the personal data stored in the video archives can be removed by operators who have the permissions for this user action.



### 6.4 Input control

The system contains two log locations:

1. The BVMS Logbook (an SQL database, with own authorization and access rights management) stores the events configured in the configuration of the system. In addition, it stores user actions (for example, when an operator calls up a camera or adds a person to a subject list) as well as system events (e.g., device disconnected or storage state failure). The BVMS Logbook itself can also be restricted in its retention time.
2. The system log files, which can be used for debugging and detailed investigations, are stored in the file system of the server or workstation (C:\Programdata\Bosch\VMS\Log). For example, [finding the source of an unauthorized login](#) requires the usage of the system log files. The retention time of the log files differs depending on the purpose of the specific log file and the application, but is typically set to 200MByte (the actual time is depending on the amount of log data being generated and therefore to the usage of the system).

### 6.5 Customer self-service

As video surveillance systems are typically not accessible for the public this section is not applicable.

### 6.6 Encryption

Information related to specific software security measures are described in the [BVMS - Securing the Security System](#) article.

### 6.7 Threshold Probability

Default: 55%; Minimum 0%; Maximum 100%

The similarity of a detected face and a reference photo in the database is expressed as a percentage between 0% and

100%. The higher this number is, the higher is the probability that the two faces are the same person. The threshold probability defines the threshold, above which the system considers it a match and triggers an alarm.

## 7 Recommendations for on-premise solutions

The [BVMS - Securing the Security System](#) recommends how to handle the system configuration from an IT security perspective, while the [BVMS Network Design](#) guide gives recommendations on how to set up the network infrastructure. Bosch recommends involving an IT security/network specialist to ensure these recommendations fit to your specific IT infrastructure.