Short Public Report

1. **Name and version of the IT product:**

   XProtect Corporate 2021 R1

2. **Manufacturer or vendor of the IT product:**

   Company Name:

   Milestone Systems A/S

   Address:

   Banemarksvej 50 C

   DK-2605 Brøndby, Denmark

   Contact Person:

   Frank Fugl (Director, Product Management)

   FFu@milestone.dk

3. **Time frame of evaluation:**

   November 2020 – July 2021

4. **EuroPriSe Experts who evaluated the IT product:**

   Name of the Legal Expert:

   Norman Bäuerle

   Address of the Legal Expert:

   PriLaTec GmbH

Alt-Friedrichsfelde 11

10315 Berlin

Germany

Name of the Technical Expert:

Björn Steinemann

Address of the Technical Expert:

PriLaTec GmbH

Alt-Friedrichsfelde 11

10315 Berlin

Germany

5. Certification Authority:

Name: EuroPriSe Certification Authority
Address: Joseph-Schumpeter-Allee 25
53227 Bonn
Germany
eMail: contact@european-privacy-seal.eu

6. Specification of Target of Evaluation (ToE):

The ToE consists of the following XProtect components:

- Smart Client
- Management Client
- Management server
- Recording server
- Media database
- Event server
- Log server
- Data collector (enabled by default but no personal data involved)
- OAuth Authorization server
- Help Function via the Documentation Portal (doc.milestonesys.com)
- Partner Insights Program

The following XProtect components are not part of the ToE:

- Milestone XProtect Mobile server (disabled by default)
- Milestone Mobile and Web client
- Milestone XProtect Access (disabled by default)
- Milestone XProtect Transact (disabled by default)
- Milestone Interconnect
- Digital Living Network Alliance integration server (DLNA)

The following features of the product are not part of the ToE either:

- Processing of audio data
- Processing of meta data
- Processing of data from input and output devices

XProtect Corporate relies on devices and IT components in the environment that are also not part of the ToE:

- Microsoft SQL server
- Microsoft Active Directory (not mandatory but strongly recommended)
- IP video cameras
- Email server

The ToE does not provide further video analysis features.

7. General description of the IT product:

XProtect Corporate is a universal Video Management Software (VMS) that allows operating small video surveillance installations with a single or few video cameras on a single site up to installations with thousands of cameras distributed over many different locations. XProtect Corporate is the enterprise version of a product family that ranges from a free community edition over different intermediary variants up to the scalable and redundant product (the ToE) for multi-site installations with distributed operation. Customers of this variant of the product line are midrange to large enterprises and public authorities of any kind. Due to the general purpose and nature of the product, its usage neither is limited to a specific industrial or public sector nor to a certain area of application.

The product is often used in installations where court proof evidence of criminal offences and fraud detection are part of the deployment requirement for a VMS. XProtect Corporate can apply digital signatures over all recordings and thus ensure that the video data has not been tampered with and can be used as evidence material.

IT-Service Aspects

Even though being an IT Product, the VMS contains two inherent IT Service aspects.

a) Online Help Portal

Milestone changed the behaviour of the help function in the Clients. By default, Operators and Administrators who call the help functionality from within the Clients are now directed to Milestone's Online Help Portal that is being opened in a web browser if the client computer has internet access. If there is no internet connection, the static help is shown as before.

b) Partner Insights Service

The Partner Insights Service collects data about plugins and other software components that are integrated with XProtect Corporate installations using Milestone Integration Platform Software Development Kit (MIP SDK). This data is collected from running VMS installations and transferred to Milestone whenever the product activates or re-activates the license.

Milestone is only interested in market information about Milestone's enterprise business partners who develop integrations and plug-ins based on the MIP SDK and which is distributed via Milestone Marketplace for these components.

However, the collected data from VMS installations may also contain information from independent software developers who are not part of Milestone Technology Partner Program, and this information may contain the names of these developers. This personal data is filtered out by Milestone's Partner Insights Service at the time of collection. Nevertheless, this processing forms an IT service aspect that Milestone is the data controller for.

8. Transnational issues:

The Windows client server architecture of the ToE is inherently built for LAN environments and a single Windows Active Directory Domain. The ToE is not

suited to be used over the internet and thus it is very unlikely that a controller will use a single installation across country borders.

The IT services listed above are implemented using services provided by companies that are subject to US law, namely

- Microsoft (Azure) providing the Infrastructure as a Service (IaaS) (1) for the VM where the Partner Insights Service is operated and (2) the hosting for the Help Function (doc.milestonesys.com) and
- Google providing Analytics for the Help Function.

Usually, the providers have no possibility to make a reference to a specific natural person/user if the product is used as described in the XProtect Corporate Privacy Guide as the technical as well as the usage data point to the corporate IT of the VMS owner. Milestone has an opt-in procedure in place regarding the analytics/usage data. The VMS users are clearly informed that this data is going to be processed by a company governed by US law if they activate the collection of usage data.

9. Tools used by the manufacturer of the IT:

The clients are Windows fat clients. The server components run on IIS as web applications or run as Windows services. The product architecture builds on Windows building blocks like Windows Communication Foundation (WCF), .NET and IIS Web server and makes use of TCP/UDP/IP communication, REST and SOAP plus WS-* protocols.

The ToE expects and uses an IT environment with the following components (which are not part of the ToE).

- Microsoft SQL server
- Microsoft Active Directory (not mandatory but strongly recommended)
- Email server

10. Edition of EuroPriSe Criteria used for the evaluation:

EuroPriSe Criteria – January 2017

EuroPriSe Commentary – May 2017

11. Evaluation methods:

In order to evaluate the ToE against the EuroPriSe Criteria the following test and audit methods have been applied:

- Review of documentation (user and administrator guides, privacy and hardening guides, security and architecture whitepapers, feature documents, legal documents etc.) and data protection relevant media (e.g. training videos)
- Interviews with the technical and legal subject matter experts for the product
- Functional and security tests of the ToE in a test environment

12. Evaluation results:

Transparent and extensive documentation

The product comes with extensive and excellent documentation, online on the company's website as well as offline documents. Especially, the Privacy Guide and the provided templates – e.g., for On-the-Spot notices or video surveillance policies – give meaningful guidance for data controllers and data processors (such as security companies operating a VMS on behalf of a controller) to act lawful, fair and transparent.

The documentation of the security features of the product is very detailed and a Hardening Guide provides information about security measures and security management beyond the means of the ToE.

Online training videos and awareness tests

Online training videos are available to make VMS operators and supervisors aware of privacy issues that come with video surveillance. The training videos are combined with an interactive online test of the taught contents.

Privacy Masking

The ToE implements a distinguishing privacy masking feature that enables controllers to respect the privacy of the people in the area under video surveillance in an exceptional manner. The combination of three feature aspects makes the privacy masking special:

- Two types of masks – "permanent" masks cannot be removed in Smart clients at all and "liftable" masks can only be lifted by authorised operators.

- Temporary on demand authorisation – authorised supervisors can entitle unauthorised operators to lift masks for a defined period of time.
- Masking of video exports – operators can export video data together with the previously applied masks and can add further masks that only come into effect for a single export.

Confidential and tamper proof video data export

Using the Smart client authorised operators can export video data with the following features:

- Encrypted video data
- Signed video data and tamper detection
- Privacy masking (see above)
- Prevention against re-export of video data
- Auditability of exports through corresponding log entries

Confidential and tamper proof transport and storage of video data

Provided that the used cameras support video transmission over https, controllers and processors can configure the ToE to guarantee encryption of video data in transit towards the ToE and between all ToE components. Additionally, all media data can be encrypted and signed before it is stored in the media database.

Anonymisation of MIP SDK integration data

The given implementation of the Partner Insights Service assures that possibly contained personal data inside the data about MIP SDK integrations from existing XProtect Corporate installations is removed from the collected data sets. This happens on the fly when the data arrives on a Virtual Machine (VM) that can only be accessed by Milestone in Microsoft's Azure cloud and that are fully under Milestone's control. Before the MIP SDK data enters the filter process it is not stored on the VM, and potentially personal data of independent software developers never leaves the volatile VM memory.

Additionally, the MIP SDK data is not only transferred over a transport secured communication path (TLS encrypted) but the data is also end-to-end encrypted because the data is collected and stored on the XProtect Management server

inside the XProtect Corporate License request file, which in turn is encrypted with a public key from Milestone that comes with the VMS installation.

13. Data flow:

The two images below illustrate the flow of personal data of VMS users and of filmed people. The data flow diagram for VMS users' data leaves aside such personal data as authentication data, authorization data and configuration data in order to not clutter the diagram. We thus have focused on audit log data and alarm data.

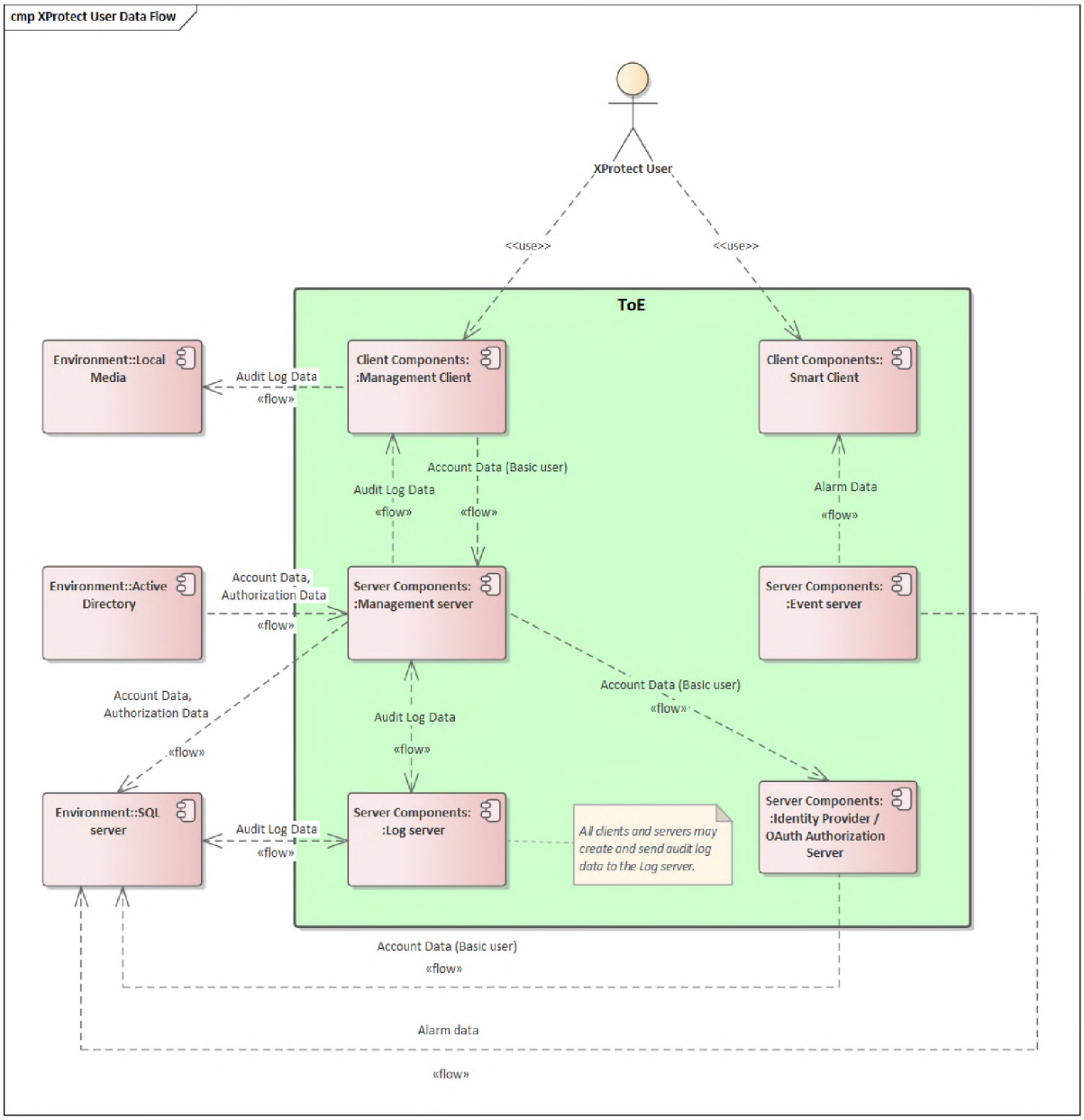

Figure 1: Components of the ToE and its environment processing XProtect Users' personal data

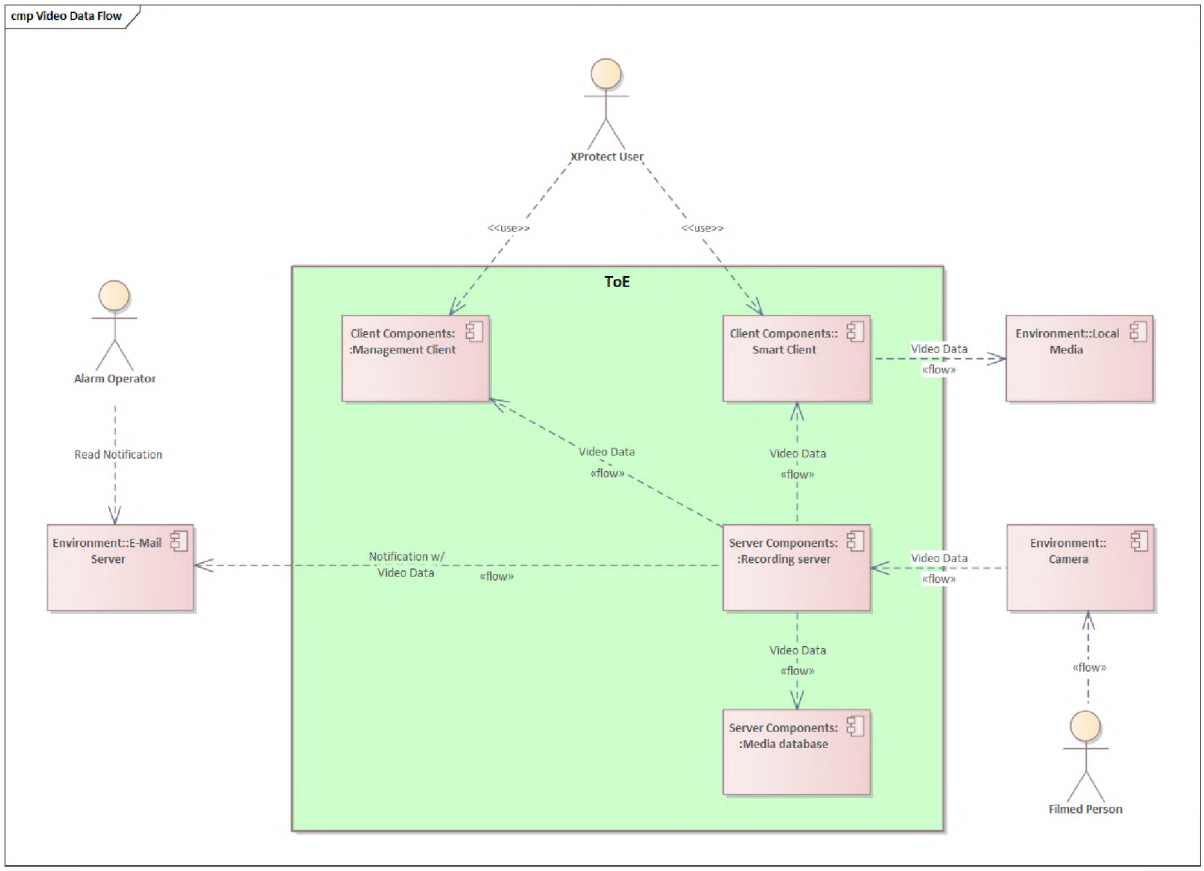

Figure 2: Components of the ToE and its environment processing video data

IT-Service Aspects

Online Help Portal

The following diagram shows the flow of personal data of VMS users visiting the Online help portal – assuming they have consented into letting Milestone set Google Analytics cookies on their computers.

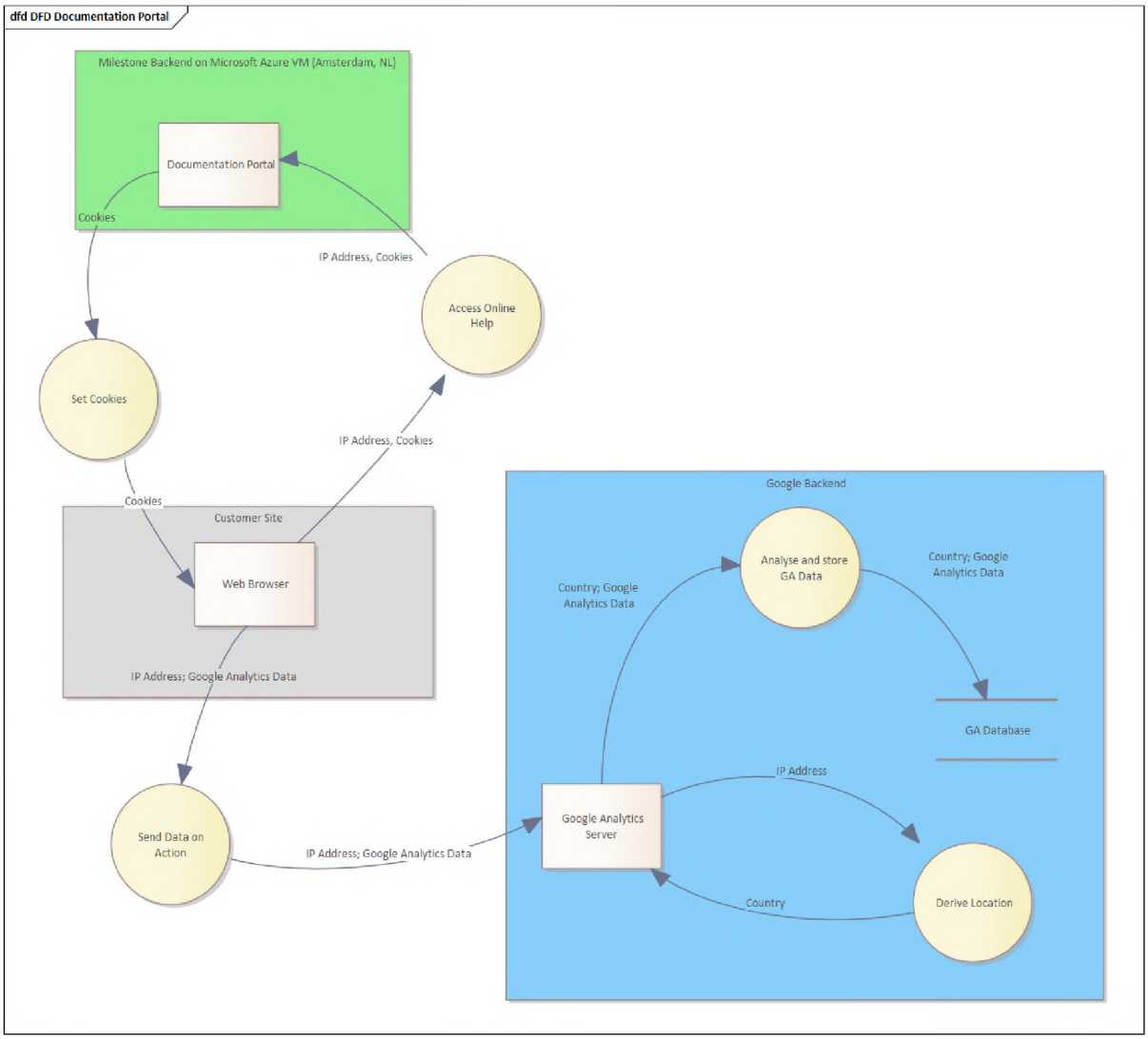

Figure 3: Data flow of personal data of Help Portal users processed with Google Analytics

Partner Insights Service

The last diagram illustrates the data flow of MIP SDK information data about integrated components, which may contain personal data.

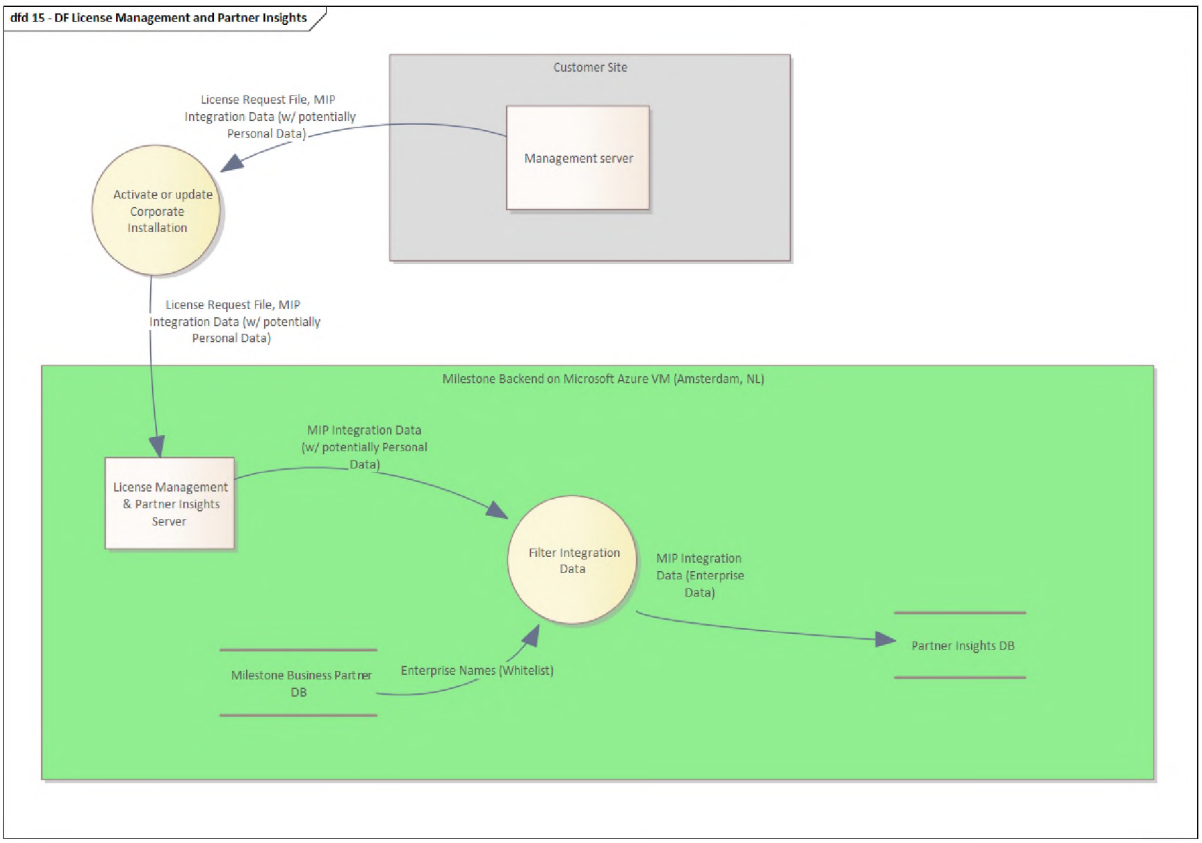

Figure 4: Deletion of potentially personal data of integration developers

14. Privacy-enhancing functionalities:

The privacy-enhancing technologies and means of the ToE have already been presented in section 12. Hence, only the most relevant aspects shall be delineated here.

- Transparent and extensive documentation of exemplary quality.
- Privacy masking that can be permanent and liftable. Authorisation to lift masks can be given temporarily and on demand to single operators.
- Video export in the XProtect format that guarantees integrity and confidentiality of the exported data. Video data is exported together with an XProtect player that prevents re-exporting of the data and additional privacy masks can be applied before the export.

15. Issues demanding special user attention:

Users of the product are required to assess the legitimacy of a video surveillance system prior to its deployment. The Privacy Guide of the ToE provides information on how to configure and operate the VMS compliant with EU data protection law.

16. Compensation of weaknesses:

Not applicable.

17. Decision table on relevant requirements:

EuroPriSe Requirement	*Decision*	*Remarks*
Data Avoidance and Minimisation	*excellent*	The ToE collects only the minimal user data that is necessary to create VMS accounts and to achieve the operation purposes. Permanent privacy masking and encrypted and signed video exports with privacy masking can reduce the processing of and access to video data significantly.
Transparency	*excellent*	The documentation provides transparent information for the controller concerning the data protection requirements that have to be adhered to when using a VMS. It comprises templates to inform the data subject of video surveillance.
Technical-Organisational Measures	*adequate*	The Privacy guide and the Hardening guide give plenty of hints to technical and organisational measures to foster data protection in video surveillance.
Data Subjects' Rights	*adequate*	The Privacy guide informs about data subjects' rights and provides information for the controller how to handle data subjects' requests.

Experts' Statement

We affirm that the above-named IT product / IT-based service has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.

Lörrach, 20.09.2021	Norman Bäuerle	
Place, Date	Name of Legal Expert	Signature of Legal Expert

Berlin, 20.09.2021	Björn Steinemann	
Place, Date	Name of Technical Expert	Signature of Technical Expert

Certification Result

The above-named IT product / IT-based service passed the EuroPriSe evaluation.

It is certified that the above-named IT product / IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

Sebastian Meissner	Digitally signed by Sebastian Meissner DN: cn=Sebastian Meissner, o=EuroPriSe GmbH, ou=EuroPriSe CA, email=meissner@european-privacy-seal.eu, c=DE Date: 2021.09.23 15:32:49 +02'00'	
Place, Date	Name of Certification Authority	Signature