31.10.2019

Short Public Report
Privacy Protector Recertification No. 05

1. Name and version of the IT product:

Privacy Protector, Version 3.2.1.0

2. Manufacturer or vendor of the IT product:

Company Name:	KiwiSecurity Software GmbH
Address:	Guglgasse 15, 1110 Vienna, Austria
Contact Person:	Dr Klemens Kraus

3. Time frame of evaluation:

12.06.2019 – 30.10.2019

4. EuroPriSe Experts who evaluated the IT:

Name of the Legal Expert:	Dr. Thomas Strohmaier
Address of the Legal Expert:	Boschstraße 55/21, 1190 Vienna, Austria
Name of the Technical Expert:	Mag. Andreas Krisch
Address of the Technical Expert:	Kirchberggasse 7/8, 1070 Vienna, Austria

5. Certification Authority:

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

6. Specification of Target of Evaluation (ToE):

KiwiSecurity's Privacy Protector is a software module for integration in a video management system.

The Privacy Protector can be called and configured by a video-framework (delivered by KiwiSecurity or third parties). The framework receives video data from surveillance cameras and hands these data over to the Privacy Protector module for obfuscation. The module analyses the incoming video data, recognises persons standing or moving within the scene and obfuscates them. The obfuscated video data is then passed to third party software systems for display and / or storage via the video framework. Different obfuscation mechanisms are available. These can be selected and configured via the video framework, which also continuously receives log data from the Privacy Protector and stores them into log files or a database. These log data do not contain any personally identifiable data.

Configuration of KiwiSecurity's Privacy Protector is carried out by KiwiSecurity or personnel specially trained and certified by KiwiSecurity. Obfuscation of video data is applied to all foreground areas (moving objects or persons). Additionally fixed regions can be defined that will always or never be obfuscated, regardless of the actual foreground. It is possible to configure multiple background models to accommodate quickly changing lighting conditions. A dedicated outdoor mode has been added to accommodate the special needs of outdoor lighting conditions.

In practice, the Privacy Protector will operate between the video signal of surveillance cameras and the picture displayed on the monitor or the storage device. Furthermore it can be used to obfuscate video data retrieved from a storage device. This results in displaying just obfuscated video data, with the monitored persons not identifiable.

The ToE includes:

- software to obfuscate video data;
- interfaces to video frameworks (input: configuration and video data, output: obfuscated video data and log data);
- a set of configuration options and mechanisms

The ToE does not include:

- hardware (cameras, servers, monitors, ...);
- video management software (display, storage, deletion, administration, access control, ... of (obfuscated) video data);
- video framework (interfaces to cameras, video management systems, configuration management and -storage, writing of log files);
- encryption of (obfuscated) video data. Encryption is optional outside the module.

Compared to the re-evaluation in 2017, the ToE has been extended by a feature to save and load background models, in order to allow for a rapid start-up when the scene is already known. While Kiwi Security also offers a video-management system and other modules for video analysis, the Target of Evaluation only covers the module Privacy Protector.

7. General description of the IT product:

The purpose of the Privacy Protector is to anonymise video data (by obfuscating persons or objects in the video) from surveillance cameras and storage devices in real-time. It also provides the possibility to define fixed obfuscated or non-obfuscated regions. To ensure a smooth functioning of the Privacy Protector, the surveillance system needs to use static surveillance cameras without automatic zoom. In case of moving cameras it is to be noted, that the Privacy Protector will obfuscate the entire scene until the new background has been learned by the software. Potential areas of operation are from highly frequented public spaces (airports, railway stations, etc.) to even working places.

Depending on the area of operation and technical settings chosen for the surveillance system, access for monitoring personnel can be restricted to obfuscated video data. Access to the non-obfuscated video data can be reserved to specially authorised users (supervisors, etc.).

8. Transnational issues:

Currently, the product is marketed especially in Austria, Belgium, Germany, Luxembourg, Netherlands and Switzerland. It is also being promoted in overseas markets such as Australia, Singapore and the USA.

9. Tools used by the manufacturer of the IT product / provider of the IT-based service:

The KiwiSecurity Privacy Protector is a software module that can be used by a video framework. Additional tools are not being used.

10. Edition of EuroPriSe Criteria used for the evaluation:

EuroPriSe Criteria Catalogue 2017/01

11. Modifications / Amendments of the IT product or IT-based service since the last (re)certification

Since the last recertification a new functionality to save background models for later reuse has been added to the certified version of the product. This functionality allows to save time on start-up and subsequent learning phases of the software.

12. Changes in the legal and/or technical situation

The GDPR and the accompanying national legislation came into effect in May 2018. This change has led to the modification and addition of a number of criteria in the EuroPriSe criteria catalogue. These changes have already been reflected in the detailed evaluation report with the recertification 2017.

The ePrivacy Directive is also being revised and can change the legal situation for future re-evaluation. This however will be of minor importance, since KiwiSecurity is promoting the Privacy Protector on a privacy friendly website that does not store IP-Addresses and refrains from the use of Cookies.

There is currently no other legal or technical change that would impact the evaluation results of the Privacy Protector compared to the re-evaluation in 2017.

13. Evaluation methods

Review of documents, review of source code, technical evaluation of the Privacy Protector website, on-site evaluation of the product based on pre-defined test-cases, interviews with the relevant representatives of the manufacturer.

14. Evaluation results

The usage of the Privacy Protector in connection with video surveillance systems permits the processing of video data while avoiding the identification of persons or objects in the surveilled area to a large extent. This is achieved by anonymisation through automatic obfuscation of video data (foreground regions) in real time.

Anonymisation:

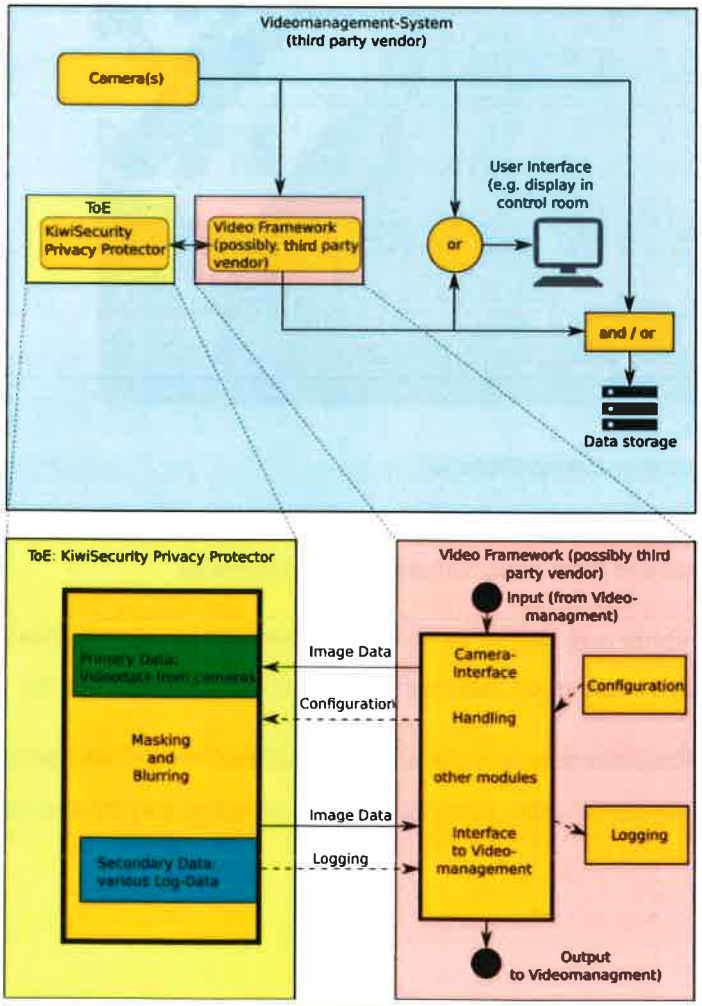
As long as non-obfuscated video data are not stored, it is possible to integrate the software into video surveillance systems, so that a re-identification of persons / objects is technically not possible. The algorithms used for obfuscating the video data all have in common that their calculations cannot be reverted.

The possibility to define fixed obfuscated or non-obfuscated regions allows a constant protection of areas that should be excluded from video surveillance (e.g. public places, working areas, sanitary areas, ...). In contrast to other video surveillance systems this allows to constantly protect privacy sensitive areas, while surveilling neighbouring areas that need special attention.

Dataminimisation / proportionality:

An immanent requirement in data protection is the usage of the least invasive technology available for achieving the purpose of the data processing. Here, KiwiSecurity's Privacy Protector significantly contributes to the protection of personal data by removing identifiable data from video sequences. Since the Privacy Protector can easily be integrated in (existing) video management systems the protection of privacy in video surveillance can be drastically enhanced with appropriate efforts.

15. Data flow:



16. Privacy-enhancing functionalities:

The Privacy Protector provides very effective algorithms for anonymisation of video data. Based on an analysis of the background present in the video data the software detects foreground objects and obfuscates (anonymises) them.

Illustration 1: Persons in a scene, obfuscated by Privacy Protector

By defining regions of the scene that should constantly be treated as foreground (these will be obfuscated), private areas can be excluded from video surveillance permanently.

Depending on the obfuscation algorithms only vague or no movements will be visible. The different available obfuscation mechanisms have in common that their calculations cannot be reverted.

As a result the usage of the Privacy Protector supports the principle of proportionality and of the usage of the least invasive technology with regard to video surveillance in an effective way by anonymization of video data and data minimisation.

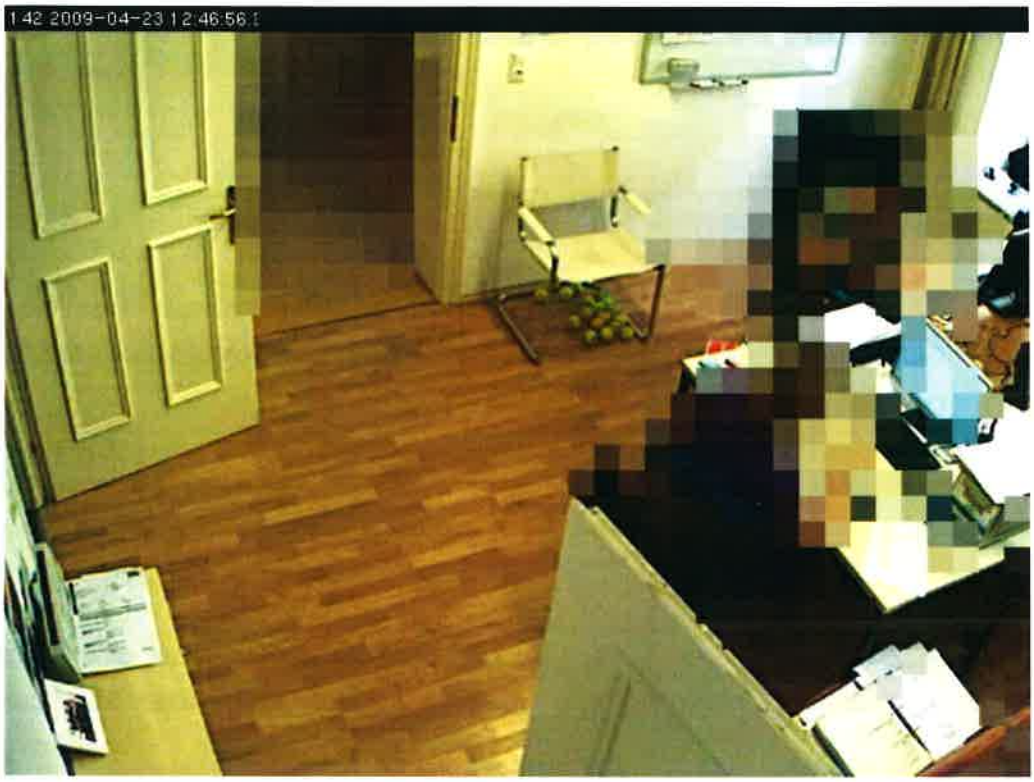


Illustration 2: Doorway on the top of the scene, permanently obfuscated by Privacy Protector

17. Issues demanding special user attention:

None of the EuroPriSe criteria was rated "additional safeguard needed"; still the legitimacy of the video surveillance system needs to be evaluated separately on a case by case basis by the operator of the video surveillance system. Customers are informed about this issue in the Kiwi Privacy Protector user manual.

The circumstances of a certain video surveillance system (camera location, recording of specific areas and events, activation of the outdoor mode in combination with dark clothing, etc.) need to be taken into account to ensure the success of the application. Therefore installation and configuration have to be carried out by especially trained personnel. The Privacy Protector user manual informs about this issue.

18. Compensation of weaknesses:

Not applicable.

19. Decision table on relevant requirements:

EuroPriSe Requirement	*Decision*	*Remarks*
Data Avoidance and Minimisation	excellent	The product anonymises video data by automatic obfuscation of persons / objects in real-time.
Transparency	excellent	The documentation is informative, up to date and understandable. It provides information for risk assessment and security policies.
Technical-Organisational Measures	adequate	All technical-organisational critera are at least fulfilled adequately. The product provides excellent anonymisation functionalities. KiwiSecurity's software release procedures provide excellent quality assurance mechanisms.
Data Subjects' Rights	adequate	According to the applicable EuroPriSe-Criteria Catalogue 2017/01 both KiwiSecurity´s website and usage of IP-addresses and cookies had to be evaluated. The result of the evaluation is that the processing is permitted.

DATEN SCHUTZ AGENTUR

Organisation Technik Compliance

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.

Vienna 30/10/2019	Dr. Thomas Strohmaier	
Place, Date	Name of Legal Expert	Signature of Legal Expert

Vienna	Mag. Andreas Krisch	
Place, Date	Name of Technical Expert	

SIGNATURINFORMATIONEN		
	Unterzeichner	Andreas Krisch
	Datum/Zeit-UTC	2019-11-21T11:54:56+01:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.	

Recertification 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: 2019.12.03 11:36:50 +01'00'

Place, Date	Name of Certification Authority	Signature