

Short Public Report

Recertification No. DE-090017

1. Name of the IT-Product:

KiwiVision Privacy Protector, Version 2.3.0.0

2. Manufacturer or vendor of the IT product:

Company Name: KiwiSecurity Software GmbH
Address: Lemböckgasse 49, 1230 Vienna, Austria
Contact Person: DI Florian Matusek

3. Time frame of evaluation:

30.05.2013 – 23.09.2013

4. EuroPriSe Experts who evaluated the IT product:

Legal Expert: Dr. Thomas Strohmaier
Address: Boschstraße 55/21, 1190 Vienna, Austria
Technical Expert: Mag. Andreas Krisch
Company: mksult GmbH
Address: Kirchberggasse 7/5, 1070 Vienna, Austria

5. Certification Body:

Name: Unabhaengiges Landeszentrum für Datenschutz - ULD
Address: Holstenstr. 98
24103 Kiel
Germany
E-Mail: europri@datenschutzzentrum.de

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 takes back 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.

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 2011, the ToE is unchanged. 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. Further countries within the European Union will follow.

9. Tools used by the manufacturer of the IT product:

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 2012/11

11. Modifications / Amendments of the IT product since the last (re)certification:

Since the last recertification there is a new option to enable multiple background models to better accommodate quickly changing lighting conditions.

12. Changes in the legal and/or technical situation

The Privacy Protector now has a new feature to compensate quick light changes in surveillance area by using several different background models. This enables a better quality for the video feed while still preserving the privacy enhancing features of the Privacy Protector.

Apart from this there have been no legal or technical changes that would impact the evaluation results of the Privacy Protector compared to the re-evaluation in 2011.

13. 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:

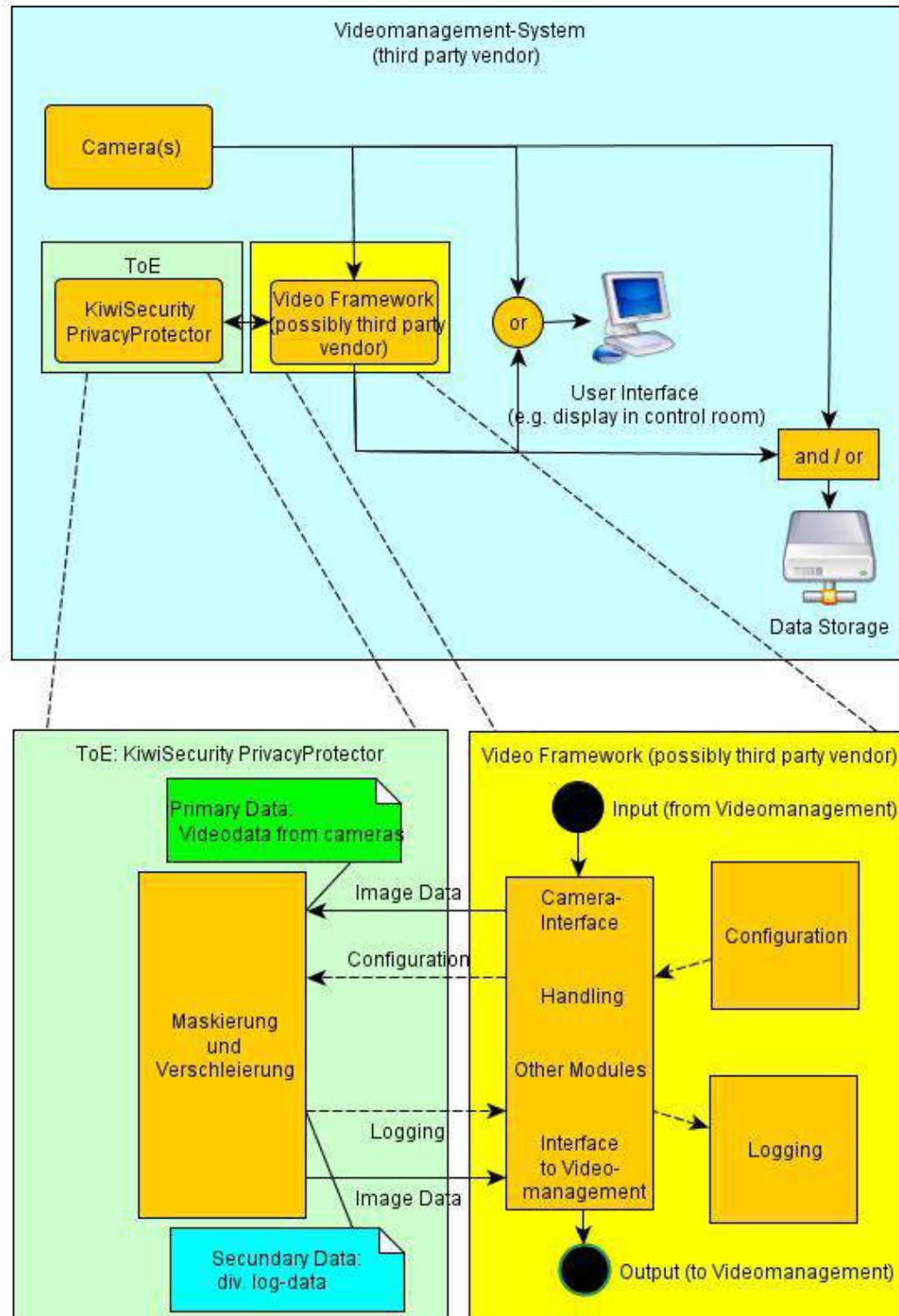
As long as non-obfuscated video data are not stored, it is possible to integrate the software into video surveillance systems, so that a re-identification of persons / objects is technically not possible. The algorithms used for obfuscating the video data all have in common that their calculations cannot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

Data minimisation / 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.

14. Data flow:



15. 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.

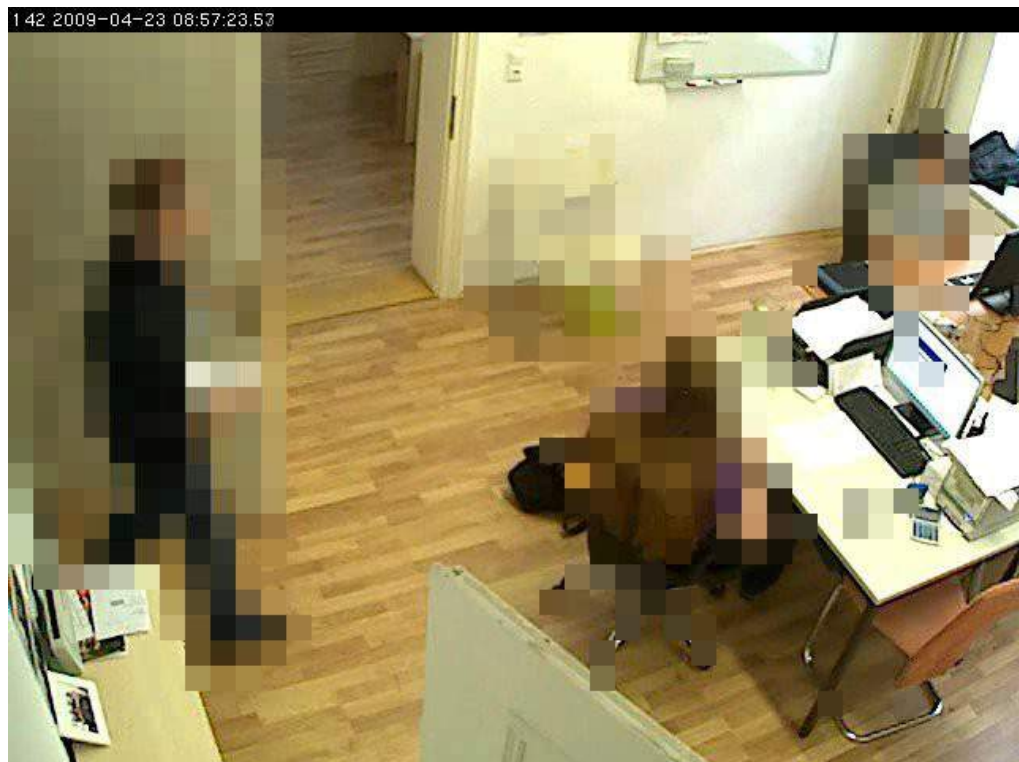


Illustration 1: Persons in a scene, obfuscated by Privacy Protector

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.

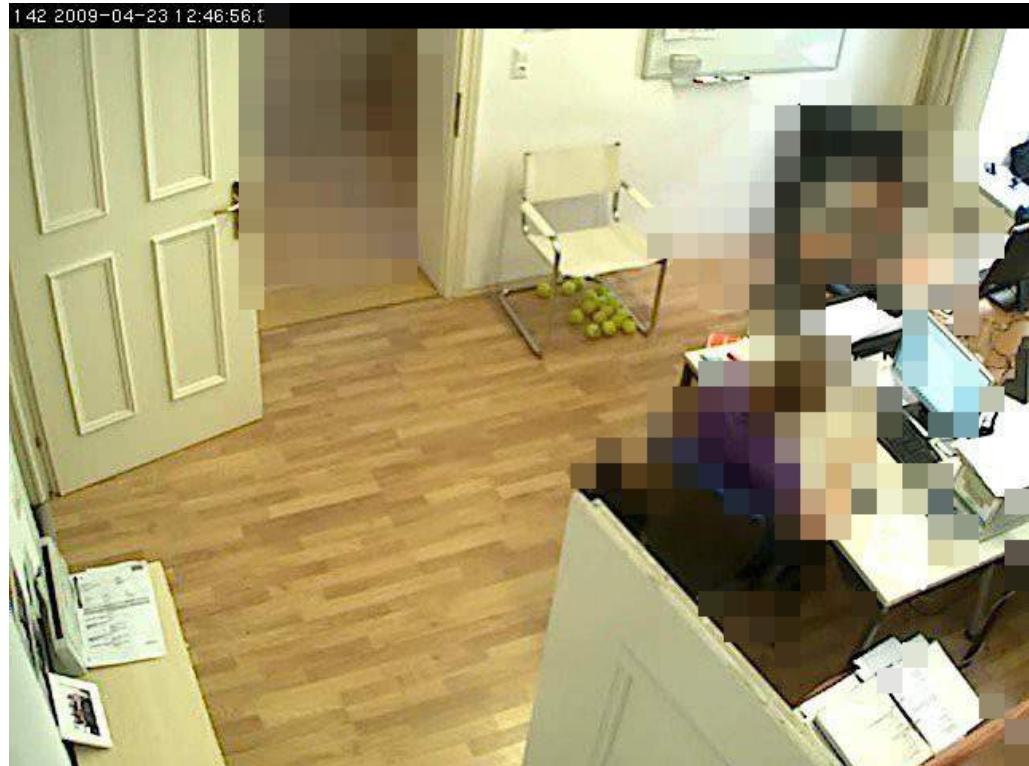


Illustration 2: Doorway on the top of the scene, permanently obfuscated by Privacy Protector

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 anonymisation of video data and data minimisation.

16. 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 KiwiVision Privacy Protector user manual.

The circumstances of a certain video surveillance system (camera location, recording of specific areas and events 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 KiwiVision Privacy Protector user manual informs about this issue.

17. Compensation of weaknesses:

Not applicable.

18. 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 criteria 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 to the applicable EuroPriSe-Criteria Catalogue 2012/11 both KiwiSecurity´s website and usage of IP-adresses and cookies had to be evaluated. In result the processing is fully permitted.

Experts' Statement

We affirm that the above-named IT product 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, 23.09..2013	Dr. Thomas Strohmaier	
Place, Date	Name of Legal Expert	Signature

Vienna, 23.09.2013	Mag. Andreas Krisch	
Place, Date	Name of Technical Expert	Signature

Recertification Result

The above-named IT product passed the EuroPriSe evaluation.

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

Place, Date	Name of Certification Body	Signature