Short Public Report

Certification No. 1 (2020/11)

1. Name and version of the IT product:

   HPD2 (Firmware Version “3.4.0b8”)

2. Manufacturer or vendor of the IT product:

   Company Name:

   Steinel GmbH

   Address:

   Dieselstraße 80-84 in 33442 Herzebrock-Clarholz, Germany

   Contact Person:

   Mr. Klaus Wördemann

3. Time frame of evaluation:

   26.05.2020 – 21.10.2020

4. EuroPriSe Experts who evaluated the IT product:

   Name of the Legal Expert:

   Mr. Jörg Schließke

   Address of the Legal Expert:

   TÜV Informationstechnik GmbH, Langemarckstraße 20, 45141 Essen, Germany

Name of the Technical Experts:

Mr. Philip Riese and Mr. Tobias Mielke

Address of the Technical Experts:

TÜV Informationstechnik GmbH, Langemarckstraße 20, 45141 Essen, 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 is HPD2. This **includes**:

- The internal data flow of HPD2
- The process of anonymization
- The web interface for administration (e.g. configuration, access)
- Ethernet, USB, and Debugging interface
- Interface to external Gateways
- Internal memory of the device

The ToE **does not include**:

- Special hardware functions (camera, sensors for temperature and humidity)
- Ethernet Hardware
- Network and Infrastructure of users of the product
- External data flow and Gateway to cloud solutions for preparing statistics

7. General description of the IT product:

The HPD2 is an optical presence detector, which detects the presence of people in a defined room. The room can also be divided into different zones, in which the persons per zone are counted separately. With this unique technology, both the presence and the exact number of people in a room can be detected precisely and in real time.

HPD2 can be used in the context of desk sharing or flexible workplaces to provide employees with an overview of (un)available desks . Furthermore, it allows the users to manage the availability of meeting rooms or to facilitate an efficient lift usage by counting the number of persons waiting for a lift. In addition, HPD2 can be used for energy management: E.g., light, heating and air-conditioning can be controlled in line with the demand resulting from the number of people present in a room. Finally, it could also be used in emergency cases to see how many people are in a room.

The core of the personal sensor is a high-precision optical system combined with a neural AI (artificial intelligence) algorithm. An integrated image analysis provides the corresponding data in real time. The image analysis, i.e. the processing of possible personal data, takes place exclusively in the device itself. The image processing carried out directly in the sensor provides information on the number of persons and their position - real personal images are not output. The HPD2 also has integrated temperature and humidity sensors.

The HPD2 (actual firmware “fwupdate-3.4.0b8”) is a self-contained system (no dependencies on cloud components) that can detect and count human torsi with the help of a camera (CMOS sensor). The manufacturer trained the integrated neural network with 150,000 positive and 7 million negative examples for an upper body. For presence detection, users can freely define different zones within a radius of 10-12 metres and an opening angle of 110° around a single HPD2. Users are able to change this at any time. For each of the individual detection zones it is possible to indicate the number of persons present in each case.

The camera images are only captured and kept available for as long as the calculation of the number of persons takes (duration<1 second). Afterwards, the images are automatically discarded and there is no possibility to change this process. Only the anonymized number of persons who are in the room or in the corresponding zones is output.

Within the Smart Workspace, the sensor does not actively send data at any time. HPD2 is regularly interrogated via the gateway component using the REST interface located on the sensor.

HPD2 can make its data available via the Ethernet interface. Here the customer has the choice between REST, MQTT or BACnet. The interfaces can be configured in the internal web interface. For maximum security, the manufacturer recommends to integrate the sensor into a separate virtual network.

Access to the sensor is protected by the following measures

- Authentication by passwords
- Automated Logout
- Brute Force Protection
- No transmission of the camera image via the Ethernet interface

Active access to the camera image by natural persons is only intended for the period of sensor configuration and zone setup via the USB port on the device. The USB interface is used during the configuration of the zones. The configuration can only be processed locally at the respective place or room and is thus clearly visible to anyone currently present there. There is no possibility to configure the zones and the access to the live image with the web interface. After configuration via USB the user can administrate the HPD2 with the web interface in the internal network of the buyer or user. The sensor is protected against unauthorized access after installation.

8. Transnational issues:

HPD2 is offered on the website of Steinel GmbH. However, no data are transferred to any other country. The data will be anonymized and processed in the internal network of the buyer or user.

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

The manufacturer uses no special tools for the IT Product.

10. Edition of EuroPriSe Criteria used for the evaluation:

Criteria from January 2017
Commentary from May 2017

11. Evaluation methods:

The evaluators used the following methods for the technical and legal evaluation:

- Review and analysis of documents provided by Steinel
    - Manual of HPD 2
    - Further documentation, listed in the documented Evaluation Concept_v0.2
    - Reviewing of website of the manufacturer www.steinel.de and https://www.steinel.de/de/lights-sensors/produkte/sensoren/optischer-sensor/hpd2-033200.html
- Technical Evaluation
    - Security Inspection of the device
        - Access image data over the listed interfaces
        - Manipulation of data on the device
        - Interfere with the traffic to the external interfaces
        - Examine the behavior if the device is working to capacity
        - Trying to attack the device via the network
    - Web interface: OWASP testing guide (Web and API Top 10)
    - Port and vulnerability scan
    - Accessing the internal memory over the interfaces
    - Test the firmware update function
    - Check Password handling
    - Check the Logfiles
    - SSL/TLS Scan
    - Check overall Transport security
    - Check Documentation
    - Anonymization of data
- Interviews with
    - Mr. Klaus Wördemann (Product Manager)
    - Mr. Christian Dust
    - Mr. Enrico Enge
    - Mr. Jan Pohanka (Development)

12. Evaluation results:

The core of the personal sensor is a high-precision optical system combined with a neural AI (artificial intelligence) algorithm. An integrated image analysis provides the corresponding data in real time. The image analysis, i.e. the processing of possible personal data, takes place exclusively in the device itself. The image processing carried out directly in the sensor provides information on the number of persons and their position.

The pictures are stored temporarily (duration <1 second) and are deleted afterwards immediately. The device does not persistently store images or other personal data. Only the anonymized information on the number of people in the zones is then indicated via the defined interfaces of the sensor. Access logs (IP addresses) and other logs for failure logging are also solely stored in volatile memory. Accordingly, the data are deleted after powering off the device.

The camera images are anonymized in a way that the information on the number of people does not allow any personal reference to be deduced. Consequently, the information, which remains after the anonymization of the camera images, does not represent personal data.

Two different roles exist via the LAN interface and an additional role via the USB interface. The basic user can only view statistics like number of detected persons or the values of the integrated sensors lux, temperature, and humidity. Additionally, the basic user can inspect the network settings of the device. The professional user can perform firmware updates, change passwords and modify the settings of the HPD2. It is possible to view the live picture of the device and to save a configuration picture in professional mode via USB interface after the input of the picture password (the manufacturer recommends to use a double password, e.g. with the works council or the data protection officer of the buyer or user). The saved configuration picture can be accessed also over LAN, but it is not possible to save a new picture.

User specific accounts do not exist. There is no inventory of granted access rights provided by the product. Access rights can solely be revoked by changing the passwords.

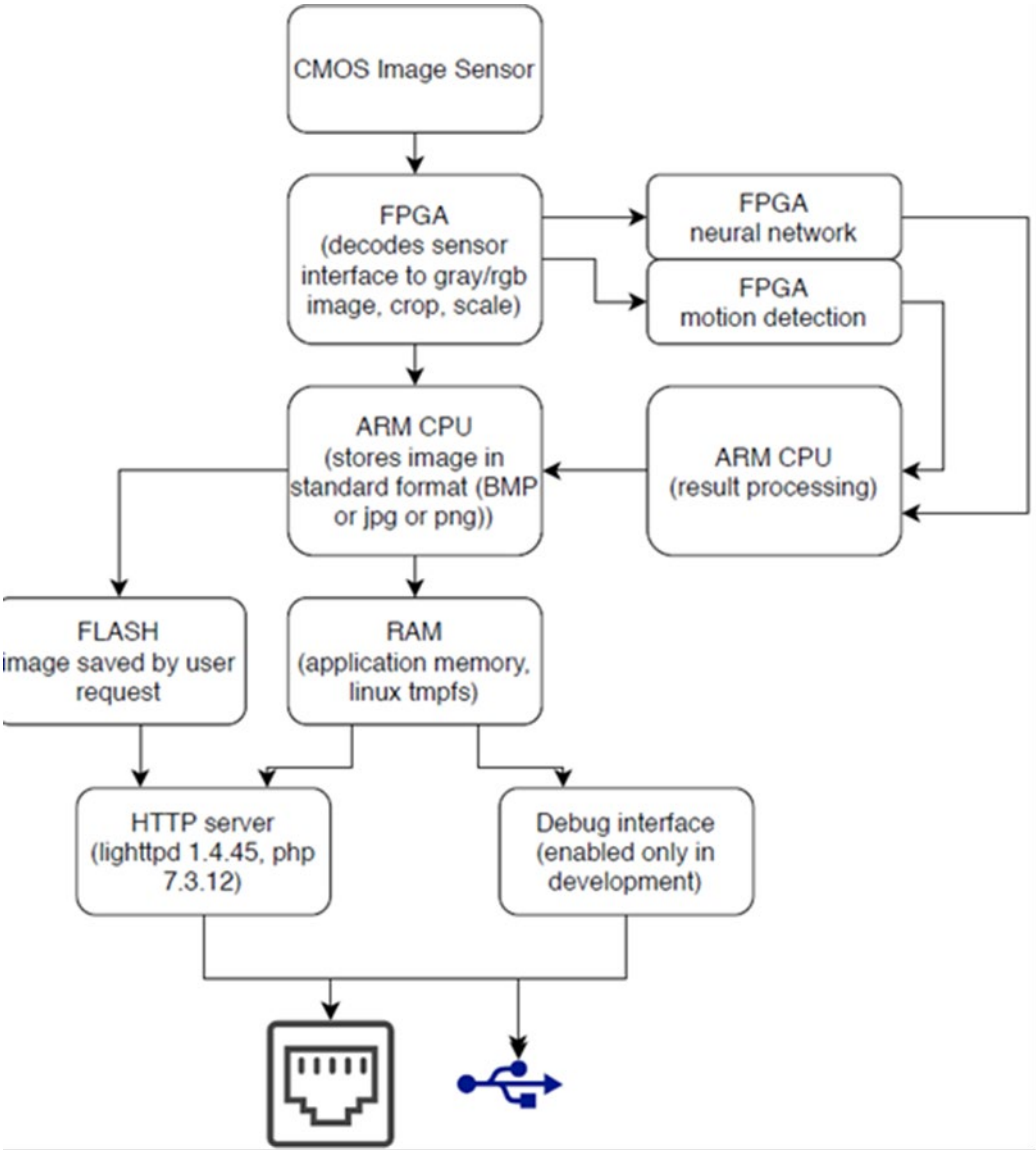
In general, the product is designed in a way that adequately complies with the general data protection principles.

The overall evaluation result is shown in the following table:

#	Set	Requirement	Evaluation result
1	1.2	Fundamental Technical Construction	excellent
2	2.1	Legal Basis for the Processing of Personal Data	processing fully permitted
3	2.2	General Requirements	adequate
4	2.3	Special Requirements to the Various Phases of the Processing	adequate
5	2.4	Special Types of Processing Operations	adequate
6	2.5	Compliance with General Data Protection Principles	adequate
7	3.1	General duties	adequate
8	3.2	Technology-specific and Service-specific Requirements	adequate
9	4.1	Rights under the General Data Protection Regulation (GDPR)	adequate
10	4.2	Rights under the ePrivacy Directive (ePD)	not applicable

13. Data flow:

The following figure shows the data flow resulting from the use of HPD2:



14. Privacy-enhancing functionalities:

The camera of the device takes pictures, which are processed by an image recognition algorithm to detect human presence. The pictures are stored temporarily and are deleted afterwards immediately. The device does not persistently store images except of the picture, which is being used during the initialization of the device and configuration of zones. Rather, it only stores image data in a volatile memory. Solely the anonymized number of persons detected can be accessed via the internal web interface of the device.

15. Issues demanding special user attention:

- Use of the double password to access the USB interface
- Using a separated internal network for the device, use the sensor only in open space and/or flex offices.
- Making sure that there are no persons in the room during the configuration of the zones (configuration picture for definition of zones)
- Inform the employees of the functions of HPD2 in context to fulfill the transparency requirements.

These hints are also part of the data protection documentation of the manufacturer.

16. Compensation of weaknesses:

Not applicable

17. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	*excellent*	The IT Product anonymises images so no personal data are processed
Transparency	*adequate*	The buyer or user is provided with a data protection documentation
Technical-Organisational Measures	*adequate*	HPD provides for anonymization of image data, connections are encrypted and data security measures are implemented (e.g., access control with double password, disconnection of USB interface after 30 minutes). HPD2 is only used in the internal network of the buyer or user
Data Subjects' Rights	adequate	The buyer or user gets a data protection information to use it for their employees

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.

Essen, 05.11.2020	Jörg Schließke	
Place, Date	Name of Legal Expert	Signature of Legal Expert

Essen, 05.11.2020	Tobias Mielke	
Essen, 05.11.2020	Philip Riese	
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: 2020.11.06 11:10:04 +01'00'
Place, Date	Name of Certification Authority	Signature