EuroPriSe European Privacy Seal

Short Public Report

1. Name and version of the IT product and IT-based service:

   Simpressive, version 2.1. ToE, functional status January 2019. simpressive is both an IT product and IT service.

2. Manufacturer or vendor of the IT product / Provider of the IT-based service:

   Company Name: *simpressive GmbH & Co. KG*

   Address: *Fahrenheitstr. 1, 28359 Bremen, Germany*

   Contact Person: *Boris Meyerdierks, CEO*

3. Time frame of evaluation: *2018-03-23 – 2019-01-23*

4. EuroPriSe Experts who evaluated the IT product or IT-based service:

   Name of the Legal Expert: *Dr. Irene Karper*

   Address of the Legal Expert: *Konsul-Smidt-Str. 88a, 28217 Bremen, Germany*

   Name of the Technical Expert: *Dr. Irene Karper*
   and until 2018-06-30 Alexey Testsov

   Address of the Technical Expert: *Konsul-Smidt-Str. 88a, 28217 Bremen, Germany*

5. Certification Body:

   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):

simpressive maps the awarding, implementation and management of purchasing processes in operation between the client and its service providers on an online platform. It is a job management tool that includes the whole service, from requirements planning and purchasing to invoicing.

Components of the ToE are:

- *IT Product „simpressive“ v. 2.1,*
- *IT Service, Subdomain *.simpressive.de, functional status January 2019,*
- *components of simpressive, which are located in the data center of Hetzner Online GmbH in Falkenstein, Germany*
- *components used by simpressive GmbH & Co. KG for the support of the service (workstations, network) as part of the contract module 6*
- *transport routes of data processing,*
- *the external interface from simpressive to the specialized processes of Mentana-Claimsoft GmbH within the framework of the interface,*

Not part of the ToE are:

- *special procedures of Mentana-Claimsoft GmbH (authentication via TAN, hardware token, video-ident as part of FP-Sign) as well as individual interfaces to systems at the user,*
- *the implementation of the software by simpressive GmbH & Co.KG (contract module 3),*
- *Consulting by simpressive GmbH & Co.KG (contract module 4)*
- *Training and workshops by simpressive GmbH & Co.KG (module 5),*
- *Later adjustments by simpressive GmbH & Co.KG (contract module 7),*
- *The IT environment of the user and his service providers,*
- *Mobile apps or other software products of simpressive GmbH & Co.KG.*

7. General description of the IT product or IT-based service:

Via simpressive, customers place their requirements on an order (for example, supplier guidelines) and manage the entire purchasing process. Per dashboard, orders can be created and viewed, content can be administrated or reports can be created. Electronic approvals can be signed (simple or qualified). Authorized users can communicate per chats in closed groups. Service providers can record project times and deposit hardskills (proof of professional competence) that may be required for the assignment of an order. Each user has an individual profile that can be viewed by authorized users.

Primary processed data include:

- first and last name of a user,
- E-mail address of a user, this may possibly contain a name of a natural person,
- time recording data of a user (employee service provider), if this function is used,
- photo in the profile of the user, if voluntarily and informed uploaded,
- username, password,
- user's hardskills with job-related evidence (such as educational, training, certification credentials, work permits) if that function is used.

Secondarily, accesses to personal data are logged and stored in a database. Also, system logs of client and server.

simpressive provides the following roles in the authorization concept:

- Employee Customer (MK))
- Representative Customer (RK))
- Representative Service Provider (RD)
- Employee Service Provider (MD)
- Administrator
- Costmanager service procider
- Data Protection Officer / Customs
- acquisition

The roles "representative service provider" and "costmanager service provider" can sign documents simple or qualified. For the purpose of protection against misuse of the digital signature, the verification takes place by entering the login data by eMail address and password or alternatively by the qualified electronic signature in the context of a two-factor authentication, which is generated via TAN. Also, hardware token- or a video ident- methods can be realized. It should *be emphasized that simpressive gives only the interface for an authentication in the context of a two-factor authentication by a local procedure, that Mentana-Claimsoft GmbH, Griesbergstr. 8, D-31162 Bad Salzdetfurth, Germany provides. The process up to the use of the interface is covered by this evaluation, but not the specialized procedure of Mentana-Claimsoft (by TAN, hardware token or video indent).*

8. Transnational issues:

   simpressive can be used by internationally operating companies. Simpressive GmbH & Co. KG and its subcontracted service providers are located in the Federal Republic of Germany. Personal data sent to clients and service providers via simpressive are employee data (representatives and employees). These data are physically processed in the data center of Hetzner Online GmbH Falkenstein in Germany.

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

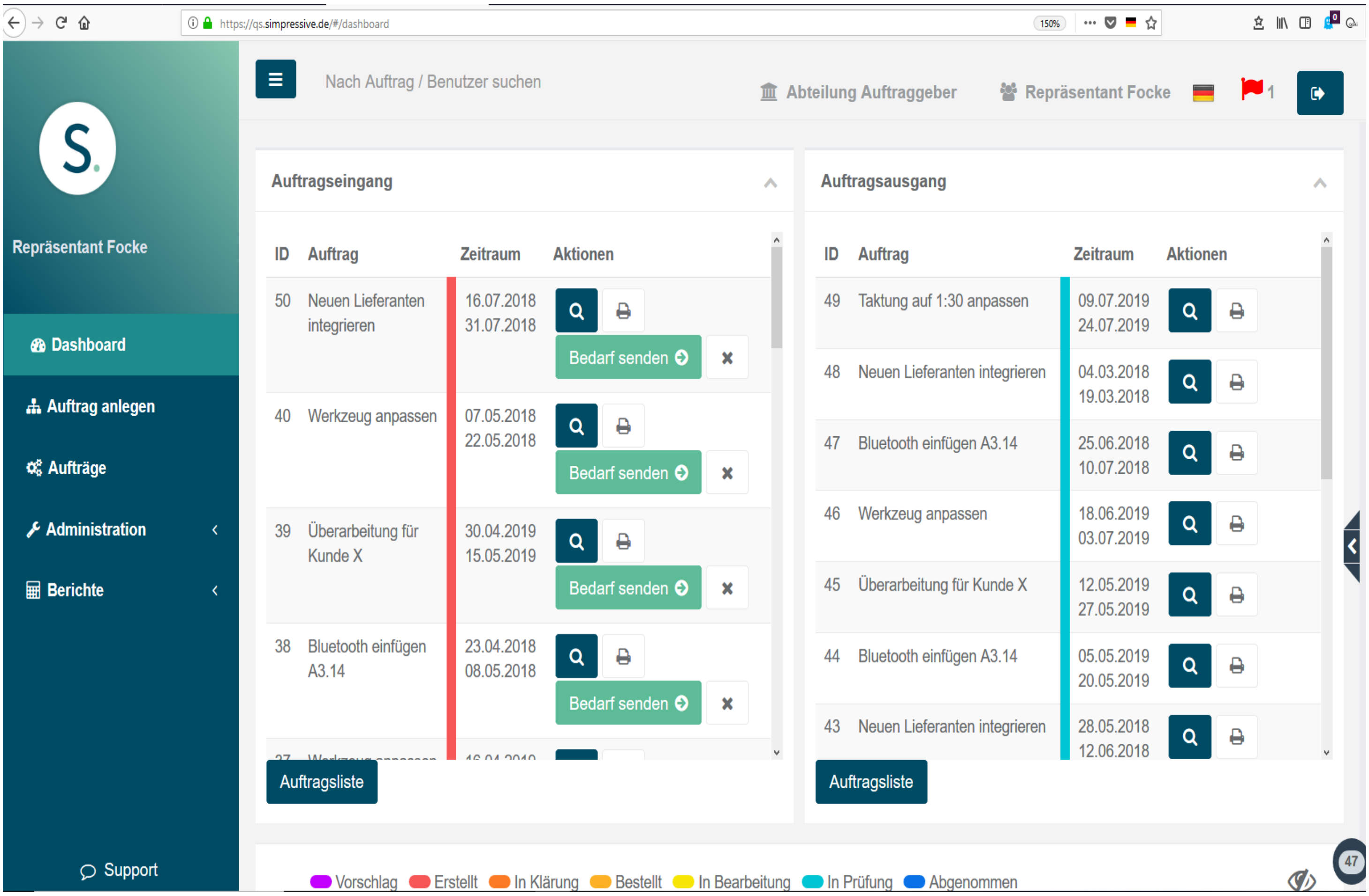
   No tools relevant to the evaluation were used.

10. Edition of EuroPriSe Criteria used for the evaluation:

    EuroPriSe-Criteria-Catalogue, January 2017.

11. Evaluation results:

    Authorized users access the login page via a subdomain (for example, https://qs.simpressive.de) that has been specially activated. After login by name and password a personal dashboard will be displayed. Here users get an overview of orders and statistics that correspond to their roles and authority.



Auftragseingang

ID	Auftrag	Zeitraum	Aktionen
50	Neuen Lieferanten integrieren	16.07.2018 31.07.2018	Bedarf senden
40	Werkzeug anpassen	07.05.2018 22.05.2018	Bedarf senden
39	Überarbeitung für Kunde X	30.04.2019 15.05.2019	Bedarf senden
38	Bluetooth einfügen A3.14	23.04.2018 08.05.2018	Bedarf senden
37	Werkzeug anpassen	16.04.2019	

Auftragsausgang

ID	Auftrag	Zeitraum	Aktionen
49	Taktung auf 1:30 anpassen	09.07.2019 24.07.2019	
48	Neuen Lieferanten integrieren	04.03.2018 19.03.2018	
47	Bluetooth einfügen A3.14	25.06.2018 10.07.2018	
46	Werkzeug anpassen	18.06.2019 03.07.2019	
45	Überarbeitung für Kunde X	12.05.2019 27.05.2019	
44	Bluetooth einfügen A3.14	05.05.2019 20.05.2019	
43	Neuen Lieferanten integrieren	28.05.2018 12.06.2018	

Illustration 1: Dashboard

simpressive mostly contains business-related data (e.g. project requirements, planning, purchasing, order data, non-personal statistics, reports, procurement guidelines). However, personal data of natural persons behind the companies and suppliers can also be processed with simpressive. These ***are employment data*** *by the means of Art. 88 GDPR, e.g. a name of the contact person, an e-Mail address (business related but, with a possibly "speaking" name), the hard skills of an employee of the supplier (e.g. certificates), time and attendance data and data related to the profile of the user (username, password and voluntarily a photo).*

Clients of projects should be regarded as ***responsible for the data processing*** *of simpressive. They initiate the tenders, project requirements, the inclusion of a service provider in the supplier management system and the project execution within the scope of the contractual service relationship. On the other hand,* ***suppliers*** *remain responsible for the processing of employment data outside of* *simpressive. If personal data of the supplier's employees is necessary for the initiation or performance of services, he shall transmit these data to the client in accordance with the data protection and employment contract specifications, e.g. name of the person employed in the project and qualifications. It should be emphasized that at the time of the evaluation, simpressive does not have any employee leasing functions*.

Legal basis of the data processing

simpressive processes data that can be assigned to an employment relationship. The legal basis is therefore the ***employment contract pursuant to Art. 6 (1) lit. b GDPR.*** *First and last name, business eMail address as well as time and attendance data, hardskills and communication via chat are processed in the course of employment and fulfilment of an employment relationship. If employees in EU member states are affected, in which the states have made use of the opening clause of Art. 88 GDPR, the country-specific regulations can be taken as a legal basis. For example, Section 26 (1) sentence 1 of the Federal Data Protection Act (FDPA) is relevant for Germany. Furthermore, collective agreements may constitute a legal basis.*

On a voluntary basis, a ***profile photo*** *can be deposited. It should be noted that in the employment relationship a voluntary and thus effective consent due to the fact of a subordinate relationship between employee and employer usually is not effective. However, the GDPR does not forbid these. Also, country-specific regulations are possible via the opening clause of Art. 88 GDPR. In Germany,* ***Section 26 (2) FDPA*** *refers to* ***consent in the employment relationship****. In order to assess the voluntary nature of the consent, particular consideration must then be given to the dependence on the employment relationship and the circumstances in which the consent was granted. In particular, voluntariness may exist if the employed person has a legal or economic advantage or if employers and employees pursue equal interests. The consent usually requires the written form. Furthermore, the employer must inform the employees about the purpose of the data processing and the right of withdrawal in text form. The German data protection authorities see an effective consent e.g. for the use of birthday lists or private use of hardware or company vehicles*[1]*.The voluntary*

[1] Cf. Short Paper No. 14 „Beschäftigtendatenschutz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK)", page. 2, 2018-01-12, https://www.datenschutz.bremen.de/sixcms/media.php/13/DSK_Nr14_Besch%E4ftigtendatenschutz.pdf (available with status from March 2019).

inclusion of a photo in simpressive as a profile picture with the consent of the employee is comparable to these exceptional circumstances. Because it does not affect the employment relationship as such, but the communication between users in simpressive. A photo in the profile can build a more personal relationship between the project participants and reduce communication barriers if necessary. This also corresponds to the equal interests of the employees and the representatives.

***Art. 6 para. 1 lit. f GDPR** can be used as a legal basis if EU member states have not made use of the opening clause of Art. 88 GDPR or if employment data is being processed which is not directly related to the work under an employee contract. In particular, the processing of **hardskills** may be warranted over the balance of interests*[2]*. Hardskills are processed in simpressive, as long as the client requires them to carry out a project, for example, because they are technically or legally necessary, e.g. with information about driving licenses or the existence of a blue card as an EU residence permission. The client can configure the required hardskills according to his needs in simpressive. **Softskills**, which are purely personal features, may not be stored in simpressive. Since the employees own their hardskills and have deliberately used or acquired them in the context of their employment relationship, it does not appear that their interests speak against processing within simpressive. On the other hand, employers and their clients have a legitimate interest in having knowledgeable and demonstrably trained personnel in their projects. Depending on the type of project, proof of blue cards may also be mandatory in accordance with the residence laws of the EU. It therefore corresponds to the legitimate interest of the parties according to Art. 6 para. 1 lit. f GDPR that this data is processed.*

*Only the employee of the service provider and, to a very limited extent, the representative of the service provider have access to **time and attendance data**. The representative of the client has no access to the information. They can only see the name of the employee involved in the order at the service provider. In addition, the time recording function should only be used if this is necessary for the project.*

[2] ibid.

Transparency:

The user is provided with a ***privacy hints sheet*** *with comprehensive information, e.g. about the data processing options, their legal classification or about privacy rights.*

Data deletion, pseudonymisation, anonymization

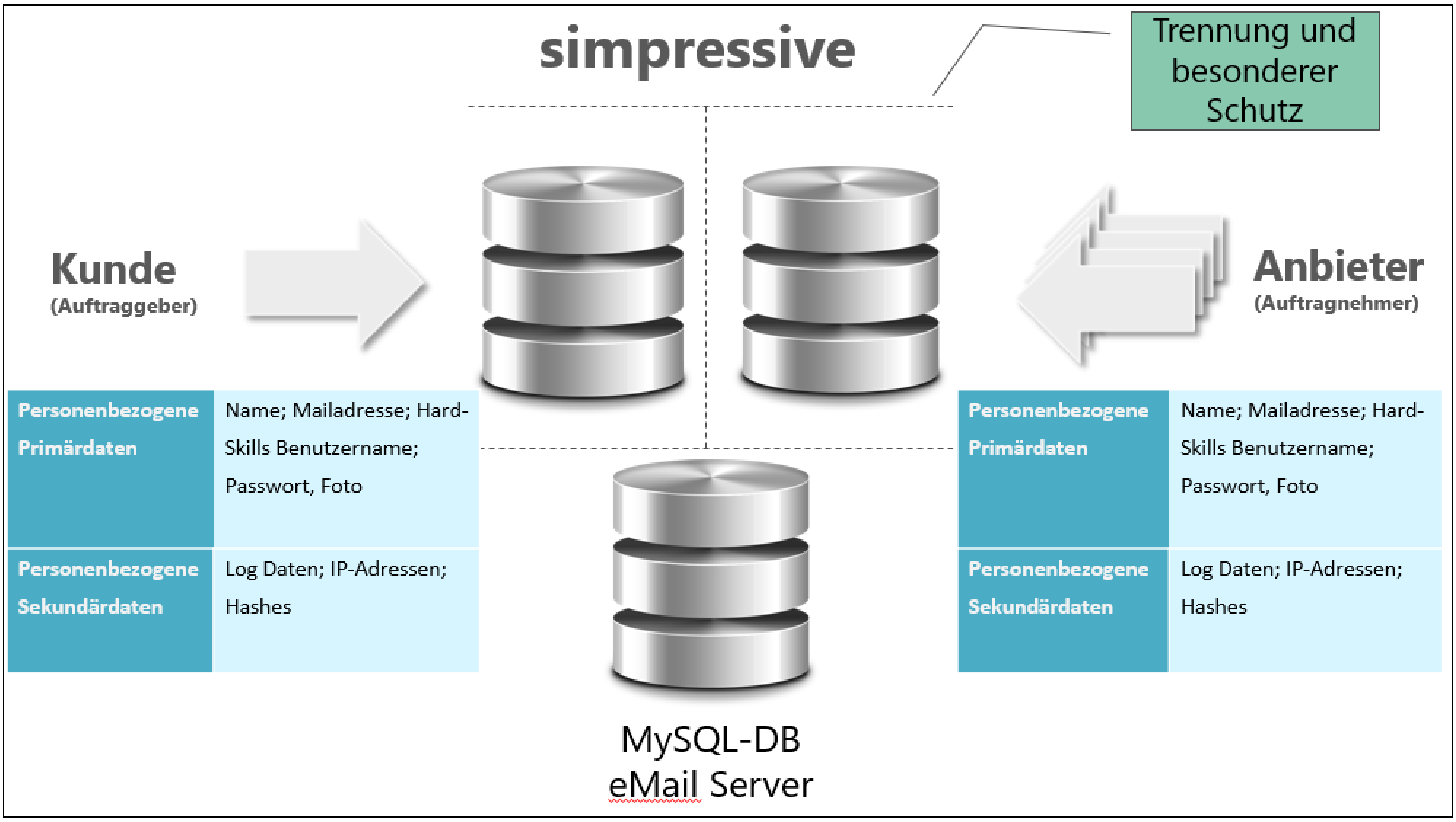
The roles Employee (MD and MK) and Representative (RD, RK) initiate the deletion of the respective data according to the regulations applicable to them or to the respective project. Furthermore, the users can initiate deletion processes in their personal profile in the account. The data are pseudonymized after the request for deletion via the administrator and kept in this form for relevant retention period until a deletion is legally possible. Data of a departing employee are pseudonymized and anonymized after the end of the retention requirements. simpressive carries out deletion processes automatically by personal data being provided with a time stamp in the course of a pseudonymization by the administrator and automatically following the expiry of the set deadline in the process of anonymization. The non-automated changeable data sets include e.g. digitally signed PDFs, which are subject to a retention period of 6 years as an order document. These are not automatically deleted, but can be deleted manually. For pseudonymization, first and last name, user name and eMail address are replaced by pseudonyms. As a result, the data are still available until deletion on schedule, e.g. for inquiries from customs or for legal disputes. Administrators can cancel the pseudonymization with the help of two keys. Access to the pseudonymised data is possible via a 4096-bit RSA key stored for the customer or his assigned service provider. The key is parted and distributed to two contracted parties or persons. This can be the customer / service provider and the simpressive GmbH & Co. KG but also e.g. be the company data protection officer. De-pseudonymization can be initiated by entering the full 4096-bit RSA key. In the case of anonymization, the personal reference is permanently removed from the data. This is done after a defined time in the system after the pseudonymization.

IT security aspects:

simpressive is offered and developed by simpressive GmbH & Co. KG as part of Software as a Service (SaaS). In individual cases, depending on the assignment, there is the possibility of providing support, whereby an insight into personal data cannot be excluded. A sample contract for order processing (Article 28 GDPR) as well as the documentation about the technical and *organizational security measures will be provided. Furthermore, the subcontractors used by the provider have been contractually obliged in accordance with Art. 28 GDPR.*

The technical and organizational data security measures implemented by the provider and its subcontractors are state of the art. simpressive is housed in a data center certified to ISO/IEC 27001. The certificate with the scope "data center infrastructure, operation and server production at the locations in Nuremberg and Falkenstein" is valid until 06.10.2019[3].

12. Data Flow:



Personenbezogene Primärdaten	Name; Mailadresse; Hard-Skills Benutzername; Passwort, Foto
Personenbezogene Sekundärdaten	Log Daten; IP-Adressen; Hashes

Personenbezogene Primärdaten	Name; Mailadresse; Hard-Skills Benutzername; Passwort, Foto
Personenbezogene Sekundärdaten	Log Daten; IP-Adressen; Hashes

Illustration 2: Data flow simpressive

13. Privacy-enhancing functionalities:

The scope of data processing by means of simpressive is tailored to the data required by the respective customer. As few as possible and at the same time only relevant data are processed.

[3] Cf.. https://www.hetzner.de/pdf/FOX_Zertifikat_de.pdf (available with status from March 2019).

In the spirit of privacy by design, functions for the implementation of information claims, the right to be forgotten, as well as data portability, anonymization and pseudonymisation were implemented in the course of development.

14. Issues demanding special user attention:

    None.

15. Compensation of weaknesses:

    Not necessary.

16. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	*excellent*	*The scope of the data processing is minimized to a few, for the project planning and execution and handling necessary personal data. The use of time tracking and hardskill matrix is optional. Softskills may not be used. When using the chat function, the user is advised in the privacy hints sheet to use only order-related data. The user is further sensitized to the most data-sparing handling of free-text fields in simpressive. Similarly, the deletion concept as well as the pseudonymization and anonymization support the limitation of a data processing to the necessary extent. The sensitivities for data economy go beyond the usual level.*
Transparency	*adequate*	*simpressive documents, in particular the privacy hints sheet, provide a clear and concise overview of the various types of data processing.*
Technical-Organisational Measures	*adequate*	*The physical and physical location of the servers of simpressive in an ISO/IEC 27001-certified data center in Germany support the high level of IT security measures.*
Data Subjects' Rights	*adequate*	*The user of simpressive is pointed out and sensitized in many places to the implementation of the affected persons rights. Also, worth mentioning is the function implemented in the system itself,*

		which allows the person concerned to simply trigger the deletion process and / or an extraction to implement the data portability.

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.

Bremen, March 07, 2019 Dr. Irene Karper Irene Karper

Place, Date Name of Legal Expert Signature of Legal Expert

Bremen, March 07, 2019 Dr. Irene Karper Irene Karper

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: 2019.05.08 11:25:25 +02'00'

Place, Date Name of Certification Authority Signature