Short Public Report

Recertification No. 1

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

   Simpressive, version 2.2. ToE, functional status December 2020. 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: *Karl-Ferdinand-Braun-Straße 5, 28359 Bremen, Germany*

   Contact Person: *Marie-Annabelle Kogge, Sales Manager,*
   simpressive GmbH & Co. KG

3. Time frame of evaluation: *01.02.2021 – 18.05.2021*

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*

   Address of the Technical Expert: *ibid*

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. 2.2,*
- *IT-based service, subdomain *.simpressive.de, functional status December 2020*
- *Components of simpressive, which are located in the data center of Hetzner Online GmbH in Falkenstein, Germany*
- *support of the service (workstations, network) by simpressive GmbH & Co. KG 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 & workshops by simpressive GmbH & Co.KG (contract module 5),*
- *Later adjustments by simpressive GmbH & Co.KG (contract module 7),*
- *The IT environment of the user and his service providers,*
- *CRM- und support ticketing tools of simpressive GmbH & Co.KG including hosting and backup by weclapp GmbH,*
- *The office of simpressive GmbH & Co. KG based in Osnabrück, Germany*

- *Services of the sub-processor Suhren,*
- *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 hard skills (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:

- *username, password,*
- *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,*
- *user's hard skills 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 are created.

simpressive provides the following roles in the authorization concept:

- *Employee Customer (MK)*
- *Representative Customer (RK)*
- *Representative Service Provider (RD)*
- *Employee Service Provider (MD)*
- *Administrator*
- *Department Administrator (new)*
- *Costmanager service provider*
- *Data Protection Officer / Customs*
- *Purchasing Department*

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 tokens or 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 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 ident).

8. Transnational issues:

   simpressive can be used by internationally operating companies. simpressive GmbH & Co. KG and its subcontracted service providers are located in 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, 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. Modifications / Amendments of the IT product or IT-based service since the last (re)certification

    simpressive has been changed in only a few points compared to the last certification:

    - *Relocation of simpressive GmbH & Co. KG to other office space within Bremen.*
    - *The simpressive tool has been slightly adapted.*
        - *The so-called user bubbles (these are the profile logos for users displayed in the account) no longer show initials at the request of the customer, but "N/A". This new feature improves pseudonymization of profiles and supports data minimization.*

- *The ISO/IEC 27001 certification of simpressive GmbH & Co. KG is still valid (regular until June 25, 2022), also for the new location.*
- *Various documents have been changed (among other things due to the new address as well as the ISO/IEC 27001 certification.*
- *The company website www.simpressive.de now contains web analytics tools from Google, implemented via a cookie banner requiring consent. The privacy policy has been adapted.*

12. Changes in the legal and/or technical situation

    None relevant.

13. Re-Evaluation methods:

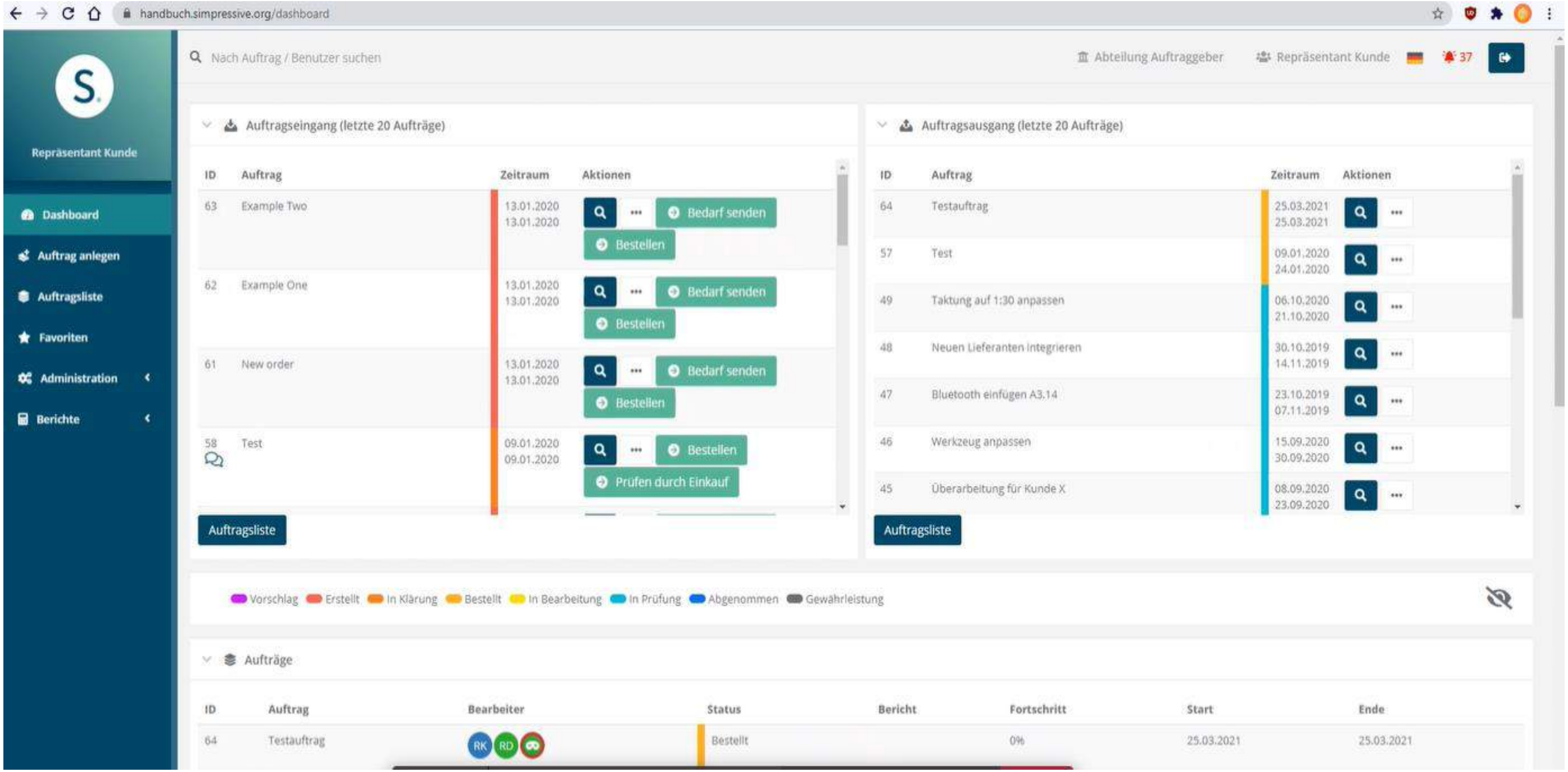
    For the evaluation, documents and the website www.simpressive.de were examined. All functions were tested in a test system via https://handbuch.simpressive.org and in a walkthrough through the test system via remote connection. Various contact persons of the company were also interviewed.

14. Re-Evaluation results:

    Authorized users access the login page via a subdomain (for example, https://handbuch.simpressive.org) that has been specially activated. After login by name and password a personal dashboard will be displayed. Here the user gets an overview of orders and statistics that correspond to his role and authority (cf. Illustration 1 below on page 6).

    simpressive mostly concerns 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 are also processed with simpressive. These ***are employee data*** *within the meaning of Art. 88 GDPR, e.g. a name of the contact person, an e-Mail address (business related but possibly with a "speaking" name), the hard skills of an employee of the supplier (e.g. certificates), time and attendance data and data in the profile of the user (username, password and voluntarily a photo).*

    Clients of projects should be regarded as ***controllers of the data processing*** *by means 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.*



handbuch.simpressive.org/dashboard

S.

Repräsentant Kunde

- Dashboard
- Auftrag anlegen
- Auftragsliste
- Favoriten
- Administration
- Berichte

Nach Auftrag / Benutzer suchen

Abteilung Auftraggeber Repräsentant Kunde 37

Auftragseingang (letzte 20 Aufträge)

ID	Auftrag	Zeitraum	Aktionen
63	Example Two	13.01.2020 13.01.2020	Bedarf senden Bestellen
62	Example One	13.01.2020 13.01.2020	Bedarf senden Bestellen
61	New order	13.01.2020 13.01.2020	Bedarf senden Bestellen
58	Test	09.01.2020 09.01.2020	Bestellen Prüfen durch Einkauf

Auftragsliste

Auftragsausgang (letzte 20 Aufträge)

ID	Auftrag	Zeitraum	Aktionen
64	Testauftrag	25.03.2021 25.03.2021	
57	Test	09.01.2020 24.01.2020	
49	Taktung auf 1:30 anpassen	06.10.2020 21.10.2020	
48	Neuen Lieferanten integrieren	30.10.2019 14.11.2019	
47	Bluetooth einfügen A3.14	23.10.2019 07.11.2019	
46	Werkzeug anpassen	15.09.2020 30.09.2020	
45	Überarbeitung für Kunde X	08.09.2020 23.09.2020	

Auftragsliste

● Vorschlag ● Erstellt ● In Klärung ● Bestellt ● In Bearbeitung ● In Prüfung ● Abgenommen ● Gewährleistung

Aufträge

ID	Auftrag	Bearbeiter	Status	Bericht	Fortschritt	Start	Ende
64	Testauftrag	RK RD	Bestellt		0%	25.03.2021	25.03.2021

Illustration 1: Dashboard

IIf 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 or relate to any employee leasing functions.

Legal basis of the data processing

simpressive tool 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, hard skills 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.*

Art. 6 para. 1 lit. f GDPR *can be used as a legal basis if employee data is being processed which is not directly related to the work under an employment contract. In particular, the processing of* ***hard skills*** *may be justified via the balancing of interests. Hard skills are processed in simpressive, if the client requires them to carry out a project. The client can configure the required hard skills according to his needs in simpressive.* ***Soft skills****, which are purely personal features, may not be stored in simpressive. Since the employees own their hard skills and have deliberately acquired them, 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. It therefore corresponds to the legitimate interest of the parties according to Art. 6 para. 1 lit. f GDPR that this data is processed. In addition, if there is a corresponding legal obligation, Art. 6 para 1 lit. c GDPR may also be considered as a legal basis (e.g. proof of blue cards according to national residence laws).*

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,*** *which may be processed, for example, on the basis of an employment contract.*

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.

Transparency:

The user is provided with a ***data protection leaflet*** *with comprehensive information, e.g. about the data processing options, their legal classification or about data subjects' 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 about 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 running them into the process of anonymization after the set deadline has expired. 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 undo 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.

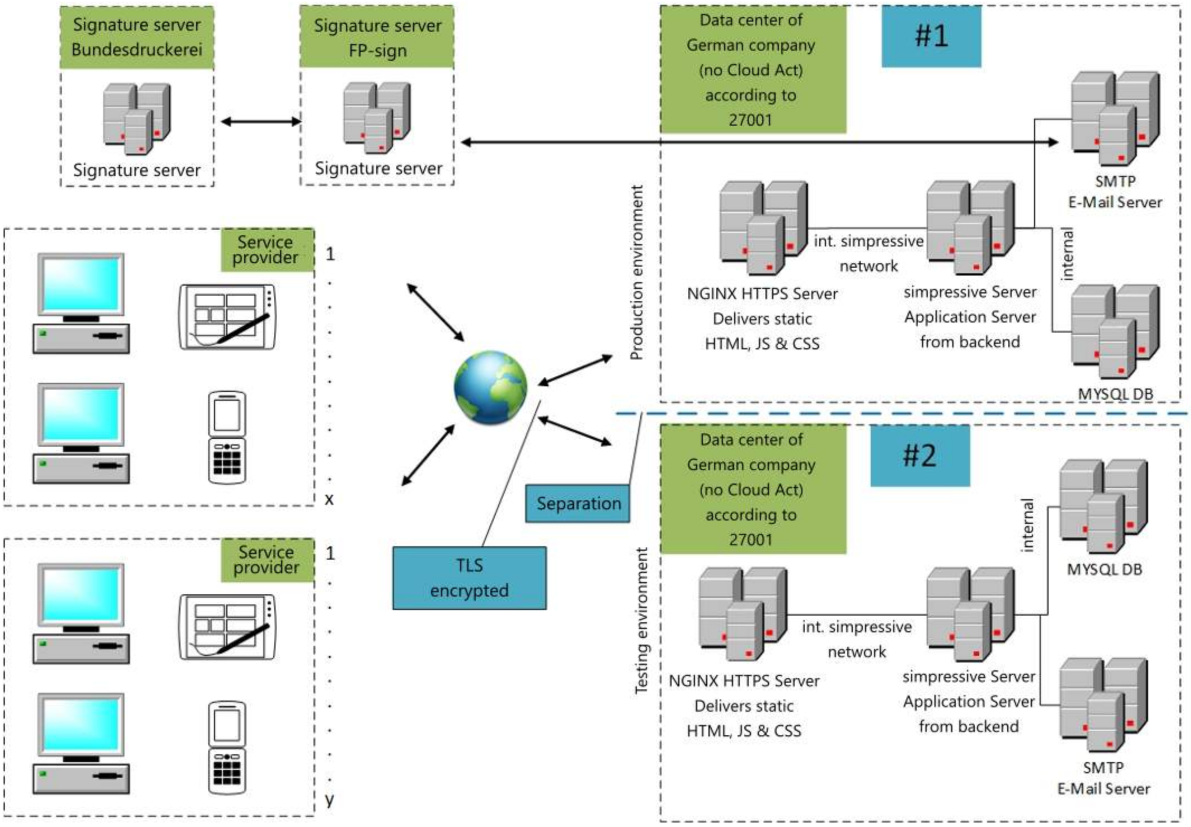
<u>IT security aspects:</u>

simpressive is offered and developed by simpressive GmbH & Co. KG as 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 data processing agreement 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.

simpressive GmbH & Co. KG has also established an ISMS that is certified by datenschutz cert GmbH in accordance with ISO/IEC 27001. The certificate under the number DSC.728.06.2019, valid until 25.06.2022, covers the scope "Secure operation, support and provision of the application "simpressive" as software-as-a-service".

15. Data Flow:



Signature server Bundesdruckerei
Signature server
Signature server FP-sign
Signature server
Data center of German company (no Cloud Act) according to 27001
#1
SMTP E-Mail Server
Production environment
int. simpressive network
internal
NGINX HTTPS Server Delivers static HTML, JS & CSS
simpressive Server Application Server from backend
MYSQL DB
Service provider
1
x
Service provider
1
y
Separation
TLS encrypted
Data center of German company (no Cloud Act) according to 27001
#2
internal
MYSQL DB
Testing environment
int. simpressive network
NGINX HTTPS Server Delivers static HTML, JS & CSS
simpressive Server Application Server from backend
SMTP E-Mail Server

Illustration 2: Data flow simpressive

16. 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.

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

17. Issues demanding special user attention:

None.

18. Compensation of weaknesses:

Not necessary.

19. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	*excellent*	*The scope of data processing is minimized to a few personal data necessary for project planning, implementation and execution. The use of time recording and hard skill matrix is optional. Softskills may not be used. When using the chat function, the user is advised in the data protection leaflet to use only order-related data. The user is further sensitized to use free-text fields in simpressive in compliance with the principle of data minimisation. Similarly, the deletion concept as well as the pseudonymization and anonymization support the limitation of data processing to the necessary extent. The sensitivities for data minimisation go beyond the usual level.*
Transparency	*adequate*	*simpressive documents, in particular the data protection leaflet, provide a clear and concise overview of the various types of data processing.*

Technical-Organisational Measures	*adequate*	*The spatial-physical location of the servers of simpressive in an ISO/IEC 27001-certified data center in Germany and the certification of the SaaS of simpressive GmbH & Co. KG support the IT security measures.*
Data Subjects’ Rights	*adequate*	*The user of simpressive is pointed out and sensitized in many places to the implementation of data subjects’ rights. Also worth mentioning is the function implemented in the system itself, which allows the data subject to simply trigger the deletion process and / or an extraction to implement 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, 24.06.2021 Dr. Irene Karper Irene Karper

Place, Date Name of Legal Expert Signature of Legal Expert

Bremen, 24.06.2021 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.

Place, Date Name of Certification Authority Signature