Short Public Report

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

   Simpressive, Versionsstand 2.1. mit Funktionsstand aus Januar 2019. simpressive ist sowohl ein IT-Produkt als auch 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, Deutschland*

   Contact Person: *Boris Meyerdierks, Geschäftsführer*

3. Time frame of evaluation: *23.03.2018 bis 23.01.2019*

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, Deutschland*

   Name of the Technical Expert: *Dr. Irene Karper sowie bis zum 30.06.2018: Alexey Testsov*

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

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 bildet die Vergabe, Durchführung und das Management von Einkaufsprozessen im Betrieb zwischen dem Auftraggeber und seinen Dienstleistern auf einer Online-Plattform ab. Es handelt sich um ein Auftrags-management-Tool, mit dem von der Bedarfsplanung über den Einkauf bis hin zur Rechnungstellung zusammengehörende Prozesse verwaltet werden.

Zum ToE gehören die Komponenten

- *IT Produkt „simpressive" v. 2.1,*
- *IT Service, Unterdomäne *.simpressive.de mit Funktionsstand Januar 2019,*
- *Die Komponenten von simpressive, die im Rechenzentrum der Hetzner Online GmbH in Falkenstein räumlich untergebracht sind,*
- *Die Komponenten, die für den Support des Services (Workstations, Netzwerk) im Rahmen des Vertragsmoduls 6 von der simpressive GmbH & Co. KG für simpressive verwendet werden,*
- *Die Transportwege der Datenverarbeitung,*
- *die externe Schnittstelle von simpressive zu den Fachverfahren der Mentana-Claimsoft GmbH im Rahmen des Interfaces,*

Nicht zum ToE gehören

- *Die Fachverfahren der Mentana-Claimsoft GmbH (Authentisierung per TAN, Hardware-Token, Video-Ident im Rahmen von FP-Sign) sowie individuelle Schnittstellen zu Systemen beim Anwender,*
- *Die Implementierung der Software durch die simpressive GmbH & Co.KG (Vertragsmodul 3),*
- *Beratung durch die simpressive GmbH & Co.KG (Vertragsmodul 4),*
- *Schulung und Workshops durch die simpressive GmbH & Co.KG (Modul 5),*
- *Spätere Anpassungen durch die simpressive GmbH & Co.KG (Vertragsmodul 7),*
- *Die Einsatzumgebung beim Anwender und den unterbeauftragten Dienstleistern,*
- *Apps und sonstige Software-Produkte der simpressive GmbH & Co.KG.*

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

Über simpressive hinterlegen Auftraggeber ihre Anforderungen an einen Auftrag (z.B. Lieferantenrichtlinien) und steuern und verwalten den gesamten Einkaufsprozess. In einem Dashboard können Aufträge angelegt und eingesehen werden, die Berechtigungen und Inhalte administriert und Reports für das Berichtswesen erstellt werden. Elektronische Freigaben können einfach oder qualifiziert signiert werden. Über Chats in Aufträgen können berechtigte Benutzer in der geschlossenen Gruppe kommunizieren, Dienstleister können in simpressive Projektzeiten erfassen und Hardskills (Nachweise über eine berufliche Befähigung) hinterlegen, die für die Vergabe eines Auftrags ggf. Voraussetzung sind. Jeder Benutzer ist dabei mit einem für die Berechtigten einsehbaren Profil hinterlegt.

Zu den primär mittels simpressive verarbeiteten Daten gehören:

- *Vor- und Nachname eines Benutzers,*
- *E-Mail-Adresse eines Benutzers, diese kann ggf. einen Namen der natürlichen Person enthalten,*
- *Zeiterfassungsdaten eines Benutzers (Mitarbeiter Dienstleister), sofern diese Funktion genutzt wird,*
- *Foto im Profil des Benutzers, sofern freiwillig und informiert hochgeladen,*
- *Benutzername, Passwort,*
- *Hardskills eines Benutzers in Form von berufsbezogenen Nachweisen (z.B. Fortbildungs-, Schulungs- und Zertifizierungsnachweise, Arbeitserlaubnisse), sofern diese Funktion genutzt wird.*

Es werden ferner sekundär die Zugriffe auf personenbezogene Daten protokolliert und in einer Datenbank gespeichert. Zusätzlich werden Systemlogs der Client und Server erstellt.

simpressive sieht folgende Rollen im Berechtigungskonzept vor:

- *Mitarbeiter Kunde (MK)*
- *Repräsentant Kunde (RK)*
- *Repräsentant Dienstleister (RD)*
- *Mitarbeiter Dienstleister (MD)*
- *Administrator*
- *Costmanager Dienstleister*
- *Datenschutzbeauftragter / Zoll*
- *Einkauf*

Die Rollen „Repräsentant Dienstleister“ und „Costmanagement Dienstleister“ können Dokumente einfach oder qualifiziert signieren. Zum Schutz vor Missbrauch der digitalen Unterschrift erfolgt die Verifizierung über ein Eingeben der Login Daten per E-Mail-Adresse und Passwort oder alternativ bei der qualifizierten elektronischen Signatur im Rahmen einer Zwei-Faktor-Authentifikation, die über das Generieren einer TAN, per Hardware-Token oder über ein Video Ident Verfahren realisiert werden kann. Es ist hervorzuheben, dass simpressive nur die Schnittstelle für eine Authentisierung im Rahmen einer Zwei-Faktor-Authentifikation durch ein dortiges Fachverfahren der Mentana-Claimsoft GmbH, Griesbergstr. 8, D-31162 Bad Salzdetfurth zur Verfügung stellt. Das Verfahren bis zur Nutzung der Schnittstelle ist von dieser Evaluation umfasst, nicht aber das Fachverfahren der Mentana-Claimsoft (per TAN, Hardware-Token oder Video-Indent).

8. Transnational issues:

   simpressive kann von international agierenden Unternehmen angewendet werden. Die simpressive GmbH & Co. KG und ihre unterbeauftragten Dienstleister befinden sich dabei in Deutschland. Personenbezogene Daten, die per simpressive an Auftraggeber und Dienstleister übermittelt werden, sind Beschäftigtendaten (Repräsentanten und Mitarbeiter). Diese Daten werden räumlich-physikalisch im Rechenzentrum der Hetzner Online GmbH in Falkenstein in Deutschland verarbeitet.

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

   Es wurden keine für die Bewertung relevanten Tools eingesetzt.

10. Edition of EuroPriSe Criteria used for the evaluation:

    EuroPriSe-Kriterienkatalog, Version Januar 2017.

11. Evaluation results:

    Berechtigte Benutzer gelangen über eine speziell für den Anwender freigeschaltete Subdomain (z.B. https://qs.simpressive.de) auf die Anmeldeseite. Nach dem Login per Name und Passwort wird ein persönliches Dashboard angezeigt. Hier erhält der Nutzer einen Überblick über Aufträge und Statistiken, die seiner Rolle und Berechtigung entsprechen.

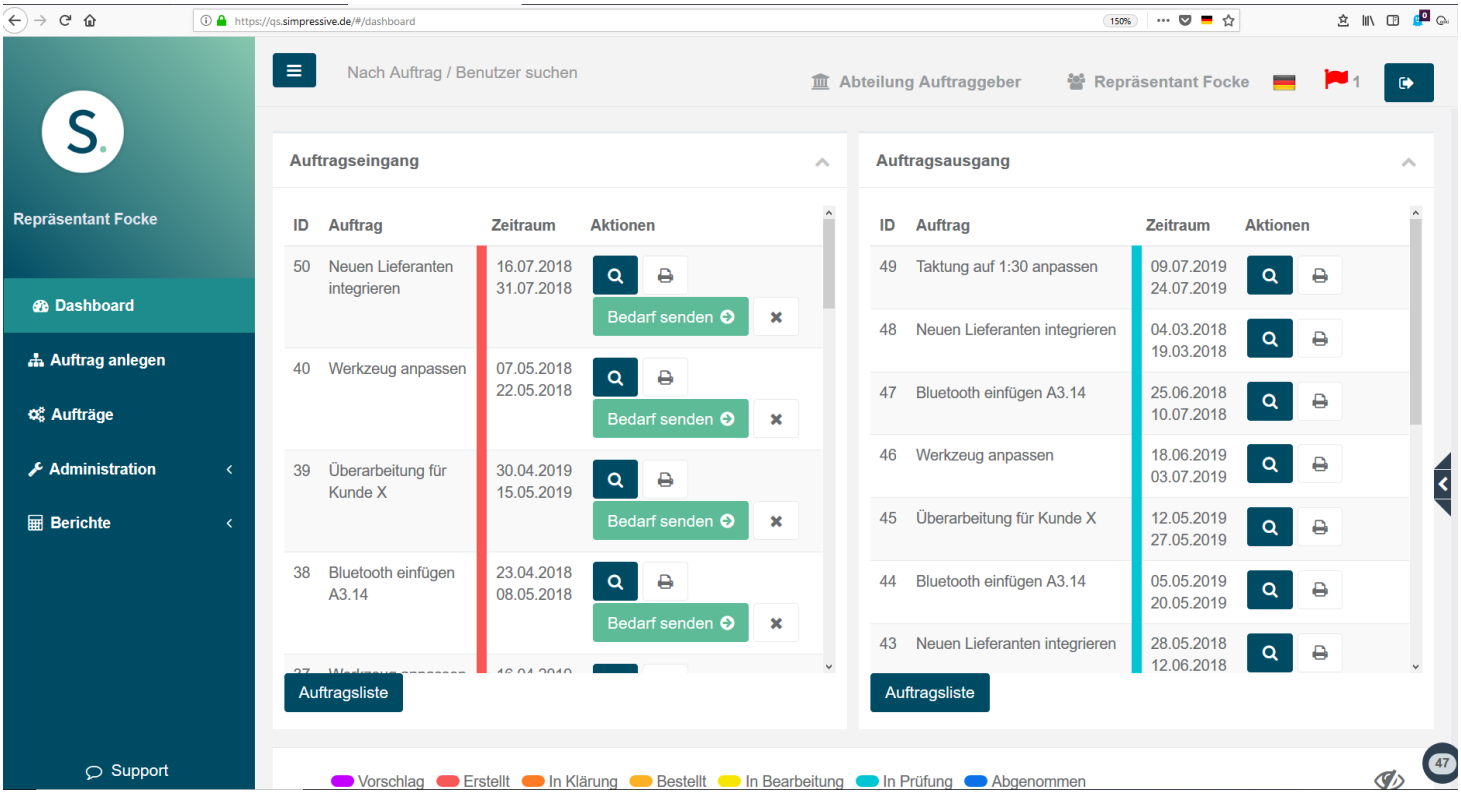

Abb. 1: Dashboard-Startseite

Bei den Verarbeitungsprozessen handelt es sich vorwiegend um geschäfts-bezogene Daten (z.B. Projektanforderungen, Planung, Einkauf, Auftragsdaten, nicht-personen-bezogene Statistiken, Berichte, Vergabe-Richtlinien). Allerdings können mit simpressive auch personenbezogene Daten der hinter den Unternehmen und Lieferanten stehenden natürlichen Personen verarbeitet werden. Dabei handelt es sich um ***Beschäftigtendaten*** *i.S.d. Art. 88 DSGVO, z.B. beim Namen des Ansprechpartners, einer E-Mail-Adresse (geschäftlich, mit ggf. „sprechenden" Namen), der Hard-Skills eines Mitarbeiters des Lieferanten (z.B. Zertifikate), der Projektzeiterfassungsdaten sowie im Profil der Benutzer (Benutzername, Passwort, sowie auf freiwilliger Basis ein Foto).*

Auftraggeber von Projekten, die simpressive nutzen, sind als ***verantwortliche Stelle*** *für die Datenverarbeitungsprozesse von simpressive anzusehen. Sie initiieren die Ausschreibungen, Projektanforderungen, die Aufnahme eines Dienstleisters in das Lieferantenmanagementsystem und die Projektabwicklung im Rahmen des vertraglichen Dienstleistungsverhältnisses. Hingegen bleiben die Lieferanten als* ***Arbeitgeber*** *verantwortliche Stelle hinsichtlich der Verarbeitung von Beschäftigtendaten außerhalb von simpressive. Sind für Anbahnung oder Durchführung von Dienstleistungen personenbezogene Daten der Beschäftigten des Lieferanten notwendig, übermittelt er diese gemäß den*

datenschutz- und arbeitsvertraglichen Vorgaben an den Auftraggeber, z.B. den Namen des im Projekt eingesetzten Beschäftigten und Befähigungsnachweise. Hervorzuheben ist, dass simpressive zum Evaluationszeitpunkt keine Arbeitsnehmerüberlassungsfunktionen aufweist oder betrifft.

<u>Rechtsgrundlagen der Datenverarbeitungen</u>

simpressive verarbeitet Projektdaten, die einem Beschäftigungsverhältnis zuzuordnen sind. Rechtsgrundlage ist daher der ***Arbeitsvertrag gemäß Art. 6 Abs. 1 lit. b DSGVO****. Vor- und Nachname, geschäftliche E-Mail-Adresse sowie Zeiterfassungsdaten oder Hardskills und die Kommunikation per Chat werden im Rahmen der Ausübung und Erfüllung eines Beschäftigungsverhältnisses verarbeitet. Sofern Beschäftigte in EU-Staaten betroffen sind, in denen die Staaten von der Öffnungsklausel des Art. 88 DSGVO Gebrauch gemacht haben, kommen die dortigen länderspezifischen Regelungen als Rechtsgrundlage in Betracht. Etwa ist für Deutschland der § 26 Abs. 1 S. 1 BDSG relevant. Ferner können Kollektivregelungen eine Rechtsgrundlage darstellen.*

Auf rein freiwilliger Basis kann ein ***Profilfoto*** *hinterlegt werden. Dabei ist zu beachten, dass im Beschäftigungsverhältnis eine freiwillige und damit wirksame Einwilligung aufgrund des bestehenden Unterordnungsverhältnisses regelmäßig nicht in Betracht kommt. Allerdings verbietet die DSGVO diese auch nicht. Vielmehr sind über die Öffnungsklausel des Art. 88 DSGVO länderspezifische Regelungen möglich. In der BRD wird in* ***§ 26 Abs. 2 BDSG*** *auf die* ***Einwilligung im Beschäftigungsverhältnis*** *Bezug genommen. Für die Beurteilung der Freiwilligkeit der Einwilligung sind danach insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf in der Regel der Schriftform. Ferner muss der Arbeitgeber die Beschäftigten über den Zweck der Datenverarbeitung und über das Widerrufsrecht in Textform aufklären. Die deutschen Datenschutzaufsichtsbehörden sehen etwa eine wirksame Einwilligung als möglich an bei Geburtstagslisten oder privater Nutzung von Hardware oder Firmenfahrzeugen*[1]*. Das freiwillige Einbringen eines Fotos in*

---

1 Vgl. Kurzpapier Nr. 14 Beschäftigtendatenschutz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), S. 2, Stand 12.01.2018, unter

simpressive als Profilbild mit Zustimmung des Beschäftigten ist mit diesen Ausnahmesachverhalten vergleichbar. Denn sie betrifft nicht das Arbeitsverhältnis als solches, sondern die Kommunikation der Benutzer untereinander in simpressive. Durch ein Foto im Profil kann eine persönlichere Beziehung der Projektbeteiligten aufgebaut und Kommunikationshindernisse ggf. abgebaut werden. Dies entspricht auch den gleichgelagerten Interessen der Mitarbeiter und der Repräsentanten.

***Art. 6 Abs. 1 lit. f DSGVO** kann als Rechtsgrundlage herangezogen werden, wenn Mitgliedstaaten der EU nicht von der Öffnungsklausel des Art. 88 DSGVO Gebrauch gemacht haben oder wenn Beschäftigtendaten verarbeitet werden, die nur in einem entfernteren Verhältnis zu den arbeitsvertraglich geschuldeten Leistungen stehen*[2]*. Insbesondere kann die Verarbeitung von **Hardskills** über die Interessenabwägung gerechtfertigt sein. Hardskills werden in simpressive verarbeitet, sofern der Auftraggeber diese für die Durchführung eines Projektes voraussetzt, etwa, weil diese fachlich oder auch gesetzlich notwendig sind. Dabei werden z.B. Angaben über Führerscheine oder das Vorliegen einer Bluecard als Aufenthaltsberechtigung in der EU erfasst. Der Auftraggeber kann die geforderten Hardskills entsprechend seiner Bedürfnisse in simpressive konfigurieren. **Softskills**, also rein persönlichen Eigenschaften, dürfen hingegen in simpressive nicht hinterlegt werden. Da die Beschäftigten Inhaber ihrer Hardskills sind und diese bewusst im Rahmen ihres Beschäftigungsverhältnisses anwenden oder erworben haben, ist nicht ersichtlich, dass ihre Interessen gegen eine Verarbeitung in simpressive sprechen. Hingegen haben Arbeitgeber und deren Aufraggeber ein berechtigtes Interesse daran, dass fachkundiges und nachweisbar geschultes Personal in ihren Projekten eingesetzt wird. Auch der Nachweis von Bluecards kann je nach Projektart gemäß den Aufenthaltsgesetzen der EU-Staaten zwingend notwendig sein. Es entspricht daher dem berechtigten Interesse der Beteiligten gemäß Art. 6 Abs. 1 lit. f DSGVO, dass diese Daten verarbeitet werden.*

*Auf **Zeiterfassungsdaten** hat nur der Mitarbeiter des Dienstleisters und in stark eingeschränktem Maß der Repräsentant des Dienstleisters Zugriff. Der Repräsentant des Auftraggebers hat keinen Zugriff auf die Informationen. Dieser kann lediglich den Namen der am Auftrag beteiligten Mitarbeiter beim Dienstleister*

---

https://www.datenschutz.bremen.de/sixcms/media.php/13/DSK_Nr14_Besch%E4ftigtendatenschutz.pdf (abrufbar mit Stand aus März 2019).

2 Ebenda.

sehen. Die Zeiterfassungsfunktion soll zudem nur genutzt werden, wenn dies für das Projekt erforderlich ist.

Transparenz:

Dem Anwender wird ein ***Datenschutzhinweisblatt*** *mit umfassenden Informationen, u.a. über die Datenverarbeitungsmöglichkeiten, deren rechtliche Einordnung oder über die Rechte der Betroffenen zur Hand gegeben.*

Datenlöschung, Pseudonymisierung, Anonymisierung

Die Rollen Mitarbeiter (MD und MK) sowie Repräsentant (RD, RK) stoßen die Löschung der jeweiligen Daten anhand der für sie bzw. für das jeweilige Projekt geltenden Bestimmungen an. Ferner können die Benutzer in ihrem persönlichen Profil im Account Löschvorgänge anstoßen. Die Daten werden nach der Löschungsaufforderung über den Administrator pseudonymisiert und nach einschlägige Aufbewahrungsfristen in dieser Form so lange aufbewahrt, bis eine Löschung rechtlich möglich ist. Die Daten eines ausscheidenden Mitarbeiters werden dabei pseudonymisiert und nach Ende der Aufbewahrungs-anforderungen anonymisiert. simpressive führt Löschvorgänge automatisiert durch, indem die personenbezogenen Daten im Zuge einer Pseudonymisierung durch den Administrator mit einem Zeitstempel versehen werden und nach Ablauf der gesetzten Frist automatisiert in den Prozess der Anonymisierung laufen. Zu den nicht automatisiert veränderbaren Datensätze gehören u.a. digital signierte PDFs; die als Auftragsdokument einer Aufbewahrungsfrist von 6 Jahren unterliegen. Diese werden nicht automatisiert gelöscht, sondern können nur manuell gelöscht werden. Für die Pseudonymisierung werden Vor- und Nachname, Benutzername und E-Mail-Adresse durch Pseudonyme ersetzt. Dadurch stehen die Daten weiterhin bis zu ihrer fristgemäßen Löschung zur Verfügung, z.B. bei Anfragen vom Zoll oder bei gerichtlichen Streitigkeiten. Administratoren können die Pseudonymisierung unter Zuhilfenahme zweier Schlüssel wieder aufheben. Der Zugriff auf die pseudonymisierten Daten ist über einen für den Kunden oder seinen beauftragten Dienstleister hinterlegten 4096-Bit RSA-Schlüssel möglich. Der Schlüssel wird dabei halbiert und an zwei vertraglich festgelegte Parteien bzw. Personen verteilt. Dies kann der Kunde/Dienstleister und die simpressive GmbH & Co. KG aber auch z.B. der betriebliche Datenschutzbeauftragte sein. Die De-Pseudonymisierung kann durch das Eingeben des vollständigen 4096-Bit RSA-Schlüssels eingeleitet werden. Bei der Anonymisierung wird der Personenbezug aus den Daten

endgültig entfernt. Dies erfolgt nach einer im System festgelegten zeitlichen Dauer nach der Pseudonymisierung.

IT-Sicherheitsaspekte:

simpressive wird seitens der simpressive GmbH & Co. KG als Software as a Service (SaaS) angeboten und entwickelt. Im Einzelfall besteht, je nach Beauftragung, die Möglichkeit, Support zu leisten, wobei dann ein Einblick in personenbezogene Daten nicht ausgeschlossen ist. Ein Mustervertrag zur Auftragsverarbeitung sowie die Dokumentation über technische und organisatorische Sicherheitsmaßnahmen werden zur Verfügung gestellt. Ferner sind die seitens des Anbieters eingesetzten Subdienstleister einer Auftragsverarbeitung gemäß Art. 28 DSGVO verpflichtet worden.

Die technischen und organisatorischen Datensicherheitsmaßnahmen, die seitens des Anbieters und seiner Subunternehmer umgesetzt werden, entsprechen dem Stand der Technik. simpressive ist in einem Rechenzentrum untergebracht, welches gemäß ISO/IEC 27001 zertifiziert ist. Das Zertifikat mit dem Scope „Rechenzentrumsinfrastruktur, -betrieb und Serverfertigung an den Standorten in Nürnberg und Falkenstein“ ist gültig bis zum 06.10.2019[3]*.*

---

3 Vgl. https://www.hetzner.de/pdf/FOX_Zertifikat_de.pdf (abrufbar mit Stand aus März 2019).

12. Data Flow:

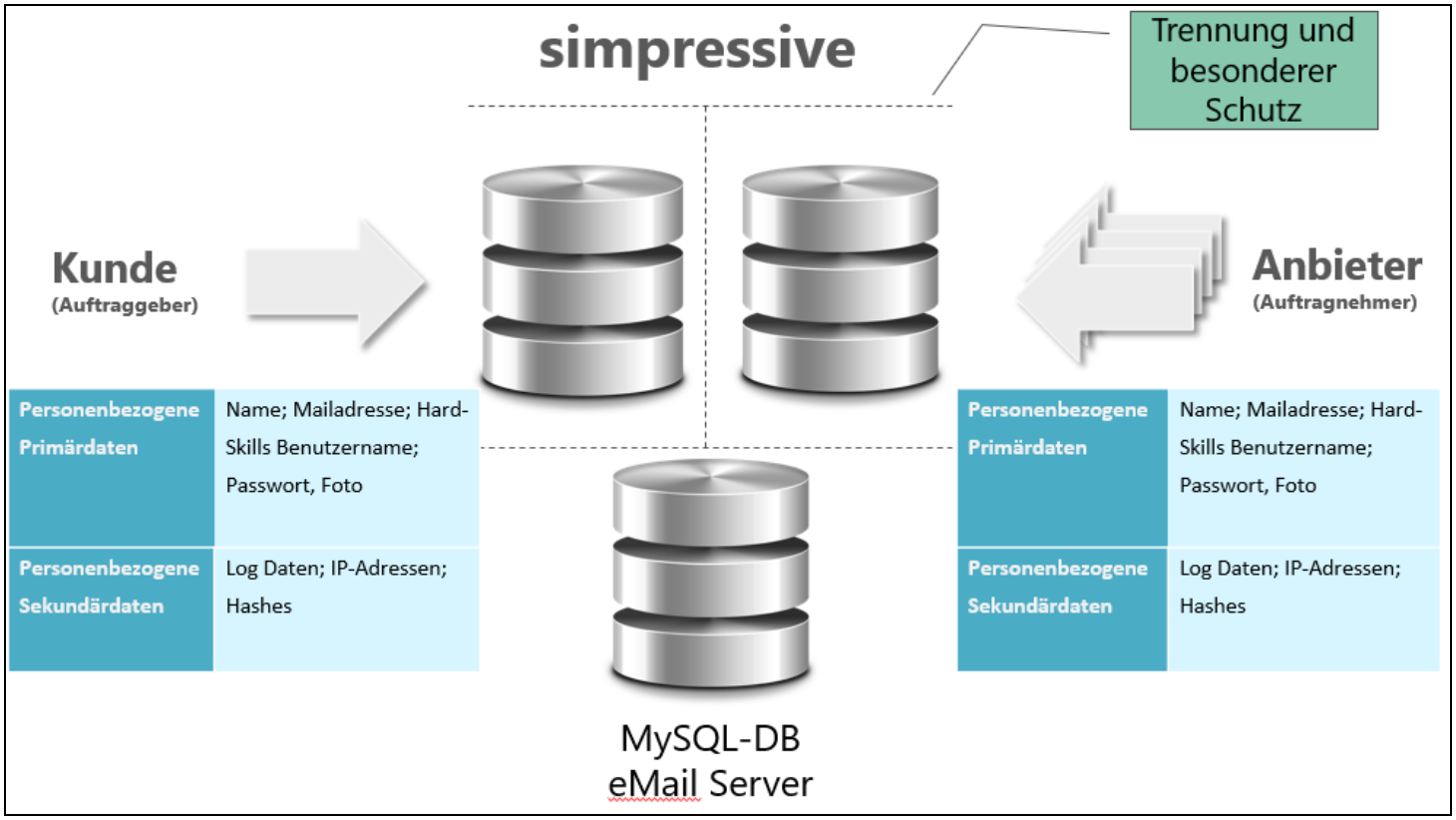

Abb. 2: Datenfluss simpressive im Überblick

13. Privacy-enhancing functionalities:

    Der Umfang der Datenverarbeitung mittels simpressive ist auf die von den jeweiligen Kunden benötigten Daten zugeschnitten. Dabei werden möglichst wenige und zugleich nur relevante Daten verarbeitet.

    Vorbildlich im Sinne des privacy by design wurden bereits im Zuge der Entwicklung Funktionen zur Umsetzung von Auskunftsansprüchen, dem Recht auf Vergessenwerden sowie der Datenportabilität, Anonymisierung und Pseudonymisierung implementiert.

14. Issues demanding special user attention:

    Keine.

15. Compensation of weaknesses:

    Nicht notwendig.

16. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	*vorbildlich*	*Der Umfang der Datenverarbeitung ist auf wenige, für die Planung, Durchführung und Abwicklung von Projekten notwendigen personenbezogenen Daten minimiert. Die Nutzung von Zeiterfassung und Hardskillmatrix ist optional. Dabei dürfen Softskills nicht verwendet werden Bei Verwendung der Chat-Funktion wird der Benutzer im Datenschutzhinweisblatt darauf hingewiesen, nur auftragsbezogene Daten zu verwenden. Der Anwender wird ferner auf den möglichst datensparsamen Umgang mit Freitextfeldern in simpressive sensibilisiert. Ebenso unterstützen das Löschkonzept sowie die Pseudonymisierung und Anonymisierung die Begrenzung einer Datenverarbeitung auf das notwendige Maß. Die Sensibilisierungen zur Datensparsamkeit gehen über das übliche Maß hinaus.*
Transparency	*angemessen*	*Dokumente zu simpressive, insbesondere das Datenschutzhinweisblatt, weisen verständlich und übersichtlich auf die verschiedenen Datenverarbeitungen hin*
Technical-Organisational Measures	*angemessen*	*Die räumlich-physikalische Unterbringung der Server von simpressive in einem ISO/IEC 27001-zertifizierten Rechenzentrum in der BRD unterstützen die hohen IT-Sicherheitsmaßnahmen.*
Data Subjects' Rights	*angemessen*	*Der Anwender von simpressive wird an vielen Stellen auf die Umsetzung der Betroffenenrechte hingewiesen und sensibilisiert. Hervorzuheben ist zudem die im System selbst implementierte Funktion, die es dem Betroffenen erlaubt, den Löschprozess und/oder eine Extraktion zur Umsetzung der Datenportabilität einfach anzustoßen*

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, den 07.03.2019 Dr. Irene Karper

Place, Date	Name of Legal Expert	Signature of Legal Expert

Bremen, den 07.03.2019 Dr. 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: 2019.05.10 10:50:42 +02'00'

Place, Date	Name of Certification Authority	Signature