Kurzgutachten

für den IT-basierten Service

REISSWOLF f.i.t.

im Auftrag der

REISSWOLF Systems GmbH
Im Hegen 13
22113 Oststeinbek

durch

Legal and Technical Expert Ann-Karina Wrede
greeneagle certification GmbH
Innungsstraße 7
21244 Buchholz
www.greeneagle-certification.de

Version 1.2

Index

1	Name und Version des IT basierten Dienstes	3
2	Adresse des Antragstellers	3
3	Zeitraum der Prüfung	3
4	EuroPriSe Expert	3
5	Zertifizierungsstelle	3
6	Spezifikation des Target of Evaluation (ToE)	4
7	Detaillierte Bezeichnung des Begutachtungsgegenstandes	5
8	Länderübegreifende Themen	5
9	Eingesetzte Komponenten	5
10	Für die Evaluation verwendete Version des EuroPriSe-Kriterienkatalogs	7
11	Zusammenfassung der Prüfergebnisse	7
12	Datenfluss	9
13	Datenschutzfördernde Gestaltung	10
14	Themen, die besondere Aufmerksamkeit fordern	10
15	Ausgleich festgestellter Schwächen	10
16	Entscheidungstabelle zu den relevanten Anforderungen	10

1 Name und Version des IT basierten Dienstes

Auditiert wurde der IT-basierte Dienst REISSWOLF f.i.t. Version 1.5, ein webbasiertes Archivierungssystem zur Datenspeicherung und zum Datenzugriff.

REISSWOLF f.i.t. ist vorrangig für den gewerblichen Einsatz konzipiert und dient dem Hochladen, Speichern, Verwalten und Austausch von Daten im Sinne eines Dokumenten-Management-Systems. Bestehende Dokumente können verwaltet, neue Dokumente hinzugefügt werden.

2 Adresse des Antragstellers

Antragstellerin der Auditierung und Zertifizierung ist die

REISSWOLF Systems GmbH
Im Hegen 13
22113 Oststeinbek

als Hersteller des IT-Produkts REISSWOLF f.i.t. und als IT-Dienstleister.
Kontaktperson ist Herr Axel Pöhlmann

3 Zeitraum der Prüfung

Die Begutachtung von REISSWOLF f.i.t. erstreckte sich auf den Zeitraum vom 30.08.-01.09.2017 vor Ort sowie im Nachgang bis 18.05.2018 und beinhaltete eine strukturierte Datenschutzanalyse auf der Basis von Interviews, der Durchführung von Tests, der Sichtung von Dokumentationen sowie Besichtigungen vor Ort.

4 EuroPriSe Expert

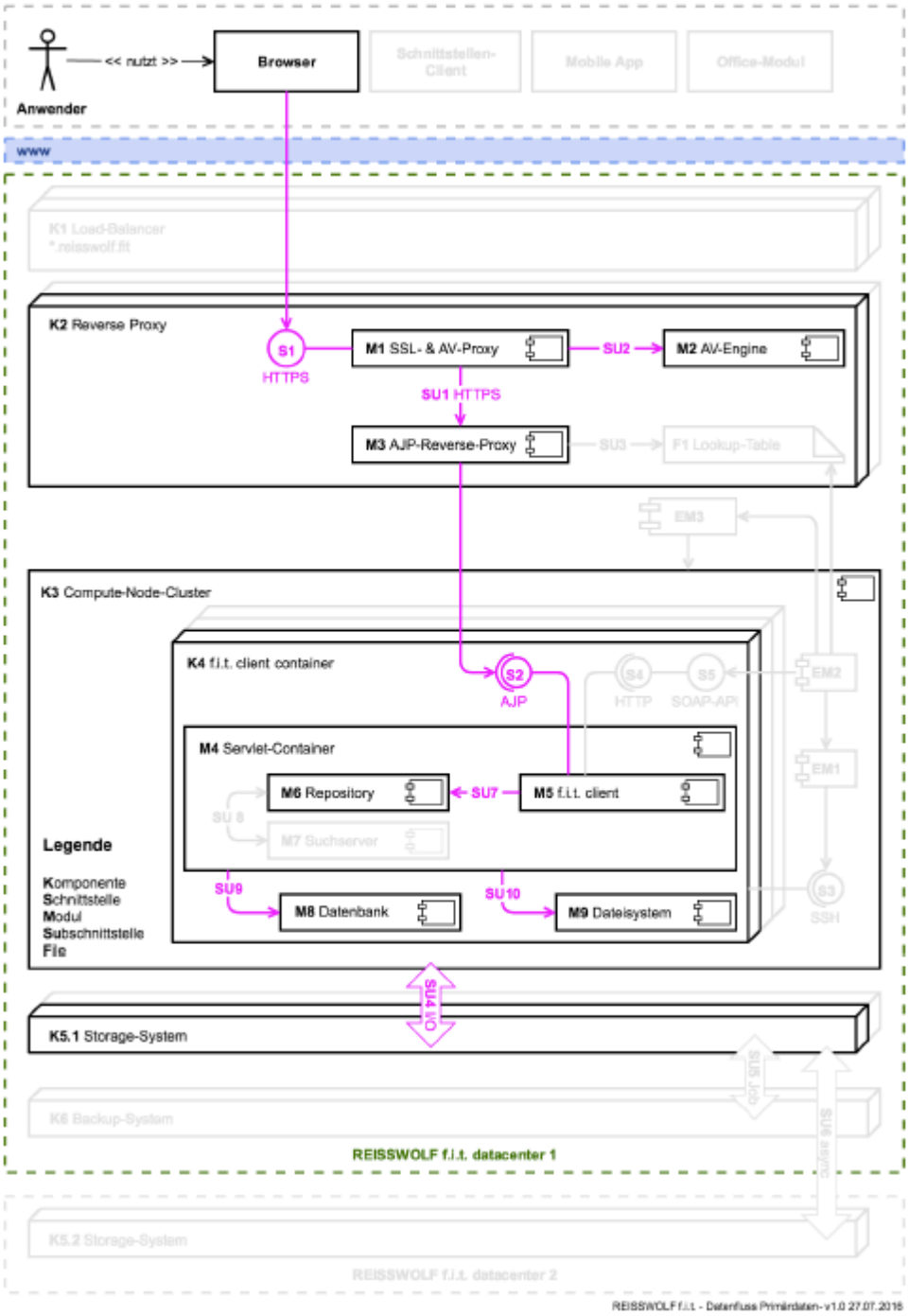
Name of the Legal and Technical Expert:
Ann-Karina Wrede

Addresse:
Beim Strohhause 17
20097 Hamburg
Tel.: 040 790 235 – 291
E-Mail: awrede@greeneagle-certification.de
Web: www.greeneagle-certification.de

5 Zertifizierungsstelle

Name: EuroPriSe Certification Authority
Address: Joseph-Schumpeter-Allee 25
53227 Bonn
Germany
eMail: contact@european-privacy-seal.eu

6 Spezifikation des Target of Evaluation (ToE)



Folgende Komponenten sind nicht Bestandteil des Zertifizierungsgegenstandes:

- REISSWOLF f.i.t Mobile App
- Office-Modul
- Teamviewer
- REISSWOLF f.i.t. hotfolder
- Sonstige alternative Client Schnittstellen

7 Detaillierte Bezeichnung des Begutachtungsgegenstandes

REISSWOLF f.i.t. ist vorrangig für den gewerblichen Einsatz konzipiert und dient dem Hochladen, Speichern, Verwalten und Austausch von Daten im Sinne eines Dokumenten-Management-Systems. Bestehende Dokumente können verwaltet, neue Dokumente hinzugefügt werden.

REISSWOLF f.i.t. wird durch REISSWOLF vertrieben und als Software as a Service (SaaS) in einem Rechenzentrum in Deutschland betrieben. REISSWOLF f.i.t. ist in Deutschland entwickelt und wird auch in Deutschland gepflegt. Das Produkt REISSWOLF f.i.t. wird weltweit angeboten und genutzt.

Der Benutzer benötigt ein personalisiertes Benutzerkonto, um mit der Arbeit beginnen zu können. REISSWOLF f.i.t. ist mit folgenden Browsern kompatibel:

- Microsoft Internet Explorer ab Version 11 (Kompatibilitätsmodus aus)
- Mozilla Firefox in der Version 35 oder neuer
- Google Chrome in der Version 40 oder neuer

Der Anwender definiert den Umfang der Zugriffsrechte auf Ordner und Dokumente selbst. Zugriffsberechtigt können z.B. interne Bereiche oder einzelne Mitarbeiter sein. Berechtigungen können pro Ordner oder Dokument an Anwender oder Gruppen vergeben werden. REISSWOLF f.i.t. stellt hierfür ein detailliert abstufbares Berechtigungskonzept zur Verfügung. Die Funktionen des REISSWOLF f.i.t. sind für den Anwender im Benutzerhandbuch transparent dokumentiert.

REISSWOLF hat keinen Einfluss auf die Art der Dokumente, die in REISSWOLF f.i.t. hochgeladen werden. Dies liegt im Verantwortungsbereich des Nutzers/ Kunden. Dieser wird allerdings über die Datenschutzhinweise im Handbuch darauf hingewiesen, dass für eine zulässige Nutzung von REISSWOLF f.i.t gegebenenfalls eine Einwilligung oder eine Schweigepflichtentbindungserklärung erforderlich sein kann.

8 Länderübegreifende Themen

REISSWOLF f.i.t. ist in Deutschland entwickelt und wird auch in Deutschland gepflegt. Das Produkt REISSWOLF f.i.t. wird weltweit angeboten und genutzt.

9 Eingesetzte Komponenten

Modul	Name	Anbieter	Typ
K1 Load-Balacer			
-	CentOS Linux	CentOS Community	Betriebssystem
-	keepalived		
K2 Reverse Proxy			
-	CentOS Linux	CentOS Community	Betriebssystem
-	Apache HTTP Server	Apache Group	Webserver
K3 Compute-Node-Cluster			

-	Virtuozzo Containers	Virtuozzo	Container Virtualisierung
K4 RW f.i.t client container			
-	Ubuntu Server	Canonical Ltd.	Betriebssystem
-	OpenJDK	Canonical Ltd.	Laufzeitumgebung
M4	Tomcat	Apache Software Foundation	Servlet Container
M8	Percona Server for MySQL	Percona LLC	Datenbank
K5 Storage-System			
-	CentOS Linux	CentOS Community	Betriebssystem
-	NFS		Fileserver
-	DRBD	LINBIT	Datenreplikation
K6 Backup-System			
-	Virtuozzo Containers	Virtuozzo	Betriebssystem
-	prlctl	Virtuozzo	Backup Software

M5 RW f.i.t. client container

Name	Anbieter	Typ
Ehcache	Terracotta, Inc.	Cache
CXF	Apache Software Foundation	Webservice-Framework
Jasypt	jasypt.org	Verschlüsselungs-Framework
Hibernate	Red Hat Community	ORM

10 Für die Evaluation verwendete Version des EuroPriSe-Kriterienkatalogs

Der Prüfung lag der Anforderungskatalogs in der Version 2.01 des ULD und die EuroPriSe Criteria von November 2011 zugrunde.

11 Zusammenfassung der Prüfergebnisse

Die rechtlichen Anforderungen in Bezug auf die Zulässigkeit der Datenverarbeitung werden eingehalten. Dies bezieht sich insbesondere auf die Einhaltung der Vorschriften nach der Richtlinie 95/46/EG.

Bei der Anmeldung und beim Betrieb von REISSWOLF f.i.t. werden die Grundprinzipen der Datensparsamkeit eingehalten:
Es wird ein Minimum von erforderlichen Daten abgefragt, um REISSWOLF f.i.t. nutzen zu können. Dabei handelt es hinsichtlich der Pflichtangaben lediglich um

- E-Mail-Adresse
- Benutzernamen (auch Pseudonyme)
- Vor- und Zuname (auch Pseudonyme)

Die übrigen Daten können durch den Nutzer freiwillig angegeben werden:

- Mobilfunknummer (nur zwingend, wenn die 2-Faktor-Authentisierung mittels SMS ausgewählt wird)
- Geheimabfrage und –antwort (nur zwingend, wenn 2-Faktor-Authentisierung hiermit ausgewählt wird)

Darüber hinaus kann als Benutzername auch ein Pseudonym genutzt werden und es muss kein realer Name ausgewählt werden.
Auch die übrigen dienstlichen Kontaktdaten (Telefonnummer, Skype for Business/ Messenger Nummer) sind freiwillige Angaben.

Im Hinblick auf die Datensicherheit sind umfangreiche Maßnahmen getroffen worden, die in der anliegenden Analyse konkret dargestellt werden. Hier sind insbesondere folgende Aspekte zur Gewährleistung der Datensicherheit zu nennen:

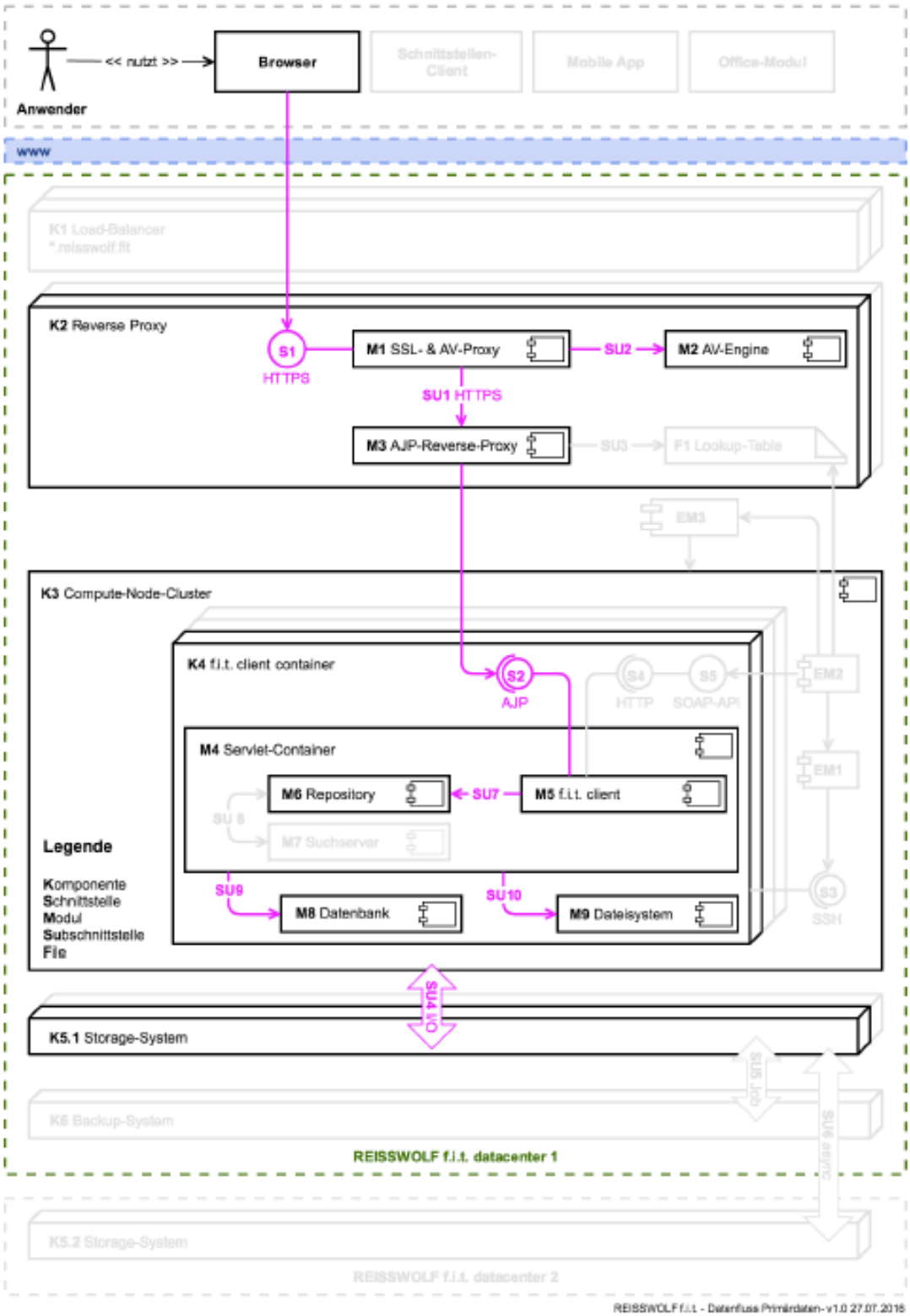
- Abgestufte Rollen- und Berechtigungskonzepte sowohl im Bereich REISSWOLF f.i.t. als auch bei den Administratoren von REISSWOLF.
- Grundsätzlich ist keine Zugriffsmöglichkeit von REISSWOLF-Administratoren auf die Container der Kunden vorgesehen und daher nur in Ausnahmefällen möglich (Ausführungen erfolgen im ausführlichen Gutachten).
- Verschlüsselte Container, pro Kunde ein Container. Mit Hilfe Virtuozzo 7 wird die Verschlüsselung der virtuellen Festplatten von Containern mittels dm-crypt und cryptsetup auf Basis einer AES-256 Verschlüsselung durchgeführt. Der Mechanismus zur Verschlüsselung ist getrennt vom Key-Management.
- Eingeschränkter Zugang zur Nutzung des Systems: Die einzige, öffentliche Schnittstelle, die dem Kunden die Nutzung des Systems ermöglicht, ist die verschlüsselte Kommunikation der Webapplikation per Browser über das HTTPS-Protokoll. Die Integrität und Sicherheit wird dabei regelmäßig über das HTTPS-Überprüfungstool von Qualys SSL Labs geprüft. Die letzte Überprüfung (11.04.2018) ergab als Prüfergebnis ein A+.

[1] Anforderungskatalog v 2.0 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH mit Stand 18.11.2014.

Im Falle einer Verschlechterung des Ergebnisses (z. B. durch die Verfügbarkeit neuer, besserer Verfahren oder bekannt gewordene Protokollschwachstellen) werden erforderliche Maßnahmen am selben Geschäftstag des Bekanntwerdens durch die Geschäftsführung veranlasst.

- Die Passwörter und Zugriffsschlüssel werden ebenfalls verschlüsselt in den jeweiligen Kunden-Containern abgelegt. Um sicherzustellen, dass nur der Anwender selbst und sonst niemand, auch kein internes System, das Passwort eines Anwenders kennen kann, werden diese einwegverschlüsselt in der Datenbank abgelegt. Es kommt das Verfahren SHA256 mit Salt und mehreren Durchläufen zum Einsatz.
- Einsatz von zertifizierten Rechenzentren über Dogado GmbH:
    - Hostway Deutschland GmbH, Hannover – ISO 27001 auf der Basis von IT-Grundschutz, BSI-IGZ-0230-2016
    - Level 3 Communications GmbH, Düsseldorf – ISO 27001, 1582475-1
- Umfangreiche Verfahrensanweisungen, Prozessbeschreibungen und Arbeitsanweisungen für Mitarbeiter von REISSWOLF.

12 Datenfluss



13 Datenschutzfördernde Gestaltung

Die Förderung des Datenschutzes erfolgt auf folgende Weise:

- Der Auslieferungszustand des Programms enthält Einstellungen die ein hohes Sicherheitsniveau garantieren. Der Benutzer wird über das Anwenderhandbuch bzw. Administrationshandbuch darauf hingewiesen, dass von einer Abweichung der eingestellten Default-Einstellungen abgeraten wird.
- REISSWOLF f.i.t. bietet ein Modul zur Zwei-Faktor-Authentisierung per SMS-TAN, welches Fremdzugriff auch bei Offenlegung von Benutzerzugängen verhindern kann.
- Über Zugriffsrichtlinien kann die Verwendung des Systems auf bestimmte Tageszeiten und/oder IP-Adressen eingeschränkt werden, um den Angriffsvektor für Fremdzugriffe zu verkleinern.
- Durch einen Tabübergreifend synchronisierten Sitzungscountdown ist der Anwender jederzeit über die tatsächliche, verbleibende Sitzungszeit in REISSWOLF f.i.t. informiert, auch wenn er in mehreren Browserfenstern oder -Tabs parallel arbeitet.
- Nur der Anwender selbst kann sein Passwort festlegen, dies gilt auch für das Initialpasswort, welches der Kunde beim Bestellen von REISSWOLF f.i.t. angibt.
- Benutzernamen können und sollen Pseudonyme sein, es besteht kein Klarnamenzwang.
- Der Anwender kann seine persönlichen Daten und sein Passwort jederzeit selbst ändern.
- Das Berechtigungskonzept von REISSWOLF f.i.t. erlaubt die Definition von Berechtigungen für Benutzer und/oder Benutzergruppen auf einzelner Ordner- und sogar Dateiebene. Auch eine Vererbung von Berechtigungen von Ordnern auf Unterordner und Dateien lässt sich bei Bedarf deaktivieren und es können neue Berechtigungen definiert werden.

14 Themen, die besondere Aufmerksamkeit fordern

Es sind keine Themen vorhanden, die eine besondere Aufmerksamkeit der Nutzer fordern.

15 Ausgleich festgestellter Schwächen

Es wurden keine Schwächen festgestellt.

16 Entscheidungstabelle zu den relevanten Anforderungen

EuroPriSe Anforderung	***Entscheidung***	***Feststellungen***
Datenvermeidung und -minimierung	*adequate*	Das Produkt nutzt die Pseudonymisierung. Darüber hinaus wird nur ein Minimum an erforderlichen Daten benötigt, um REISSWOLF f. i. t. nutzen zu können.

Tranzparenz	*adequate*	Die Dokumentation und Datenschutzbestimmungen sind informativ, aktuell und verständlich. Darüber hinaus ist für den einzelnen Nutzer jederzeit transparent, welche Daten von ihm im REISSWOLF f. i. t. an welcher Stelle verarbeitet werden.
Technische und organisatorische Maßnahmen	*adequate*	Verschlüsselte Container, ein Container pro Kunde, basierend auf AES-256-Verschlüsselung. Einsatz von zertifizierten Rechenzentren. Abgestufte Rollen- und Berechtigungskonzepte.
Betroffenenrechte	*adequate*	Die Einhaltung der Rechte der betroffenen Personen liegt weitgehend in der Verantwortung des Kunden. Darüber hinaus ist für den einzelnen Nutzer jederzeit transparent, welche Daten von ihm selbst im REISSWOLF f. i. t. an welcher Stelle verarbeitet werden.

Experts' Statement

Ich bestätige, dass die oben genannte IT-basierte Dienstleistung nach den EuroPriSe-Kriterien, -Regeln und -Prinzipien bewertet wurde und dass die oben beschriebenen Ergebnisse das Ergebnis dieser Bewertung sind.

Digital unterschrieben von Ann-Karina Wrede
DN: cn=Ann-Karina Wrede, email=awrede@greeneagle-certification.de, c=DE
Datum: 2018.06.18 07:55:38 +02'00'

Hamburg, 18.06.2018	Ann-Karina Wrede	
Place, Date	Name of Legal and Technical Expert	Signature of Expert

Certification Result

Der oben genannte IT-basierte Service hat die EuroPriSe-Bewertung bestanden.
Es wird bescheinigt, dass das oben genannte IT-Produkt / der oben genannte IT-basierte Dienst die Nutzung dieses Produkts oder Dienstes in Übereinstimmung mit den europäischen Datenschutzbestimmungen ermöglicht.

Place, Date	Name of Certification Authority	Signature