Kombiverfahren ULD und EuroPriSe

Kurzgutachten zur Erteilung eines Datenschutz-Gütesiegels

für das IT-Produkt

REISSWOLF f.i.t.

im Auftrag der

REISSWOLF Systems GmbH
Im Hegen 13
22113 Oststeinbek

durch

Sachverständige Prüfstelle (Recht und Technik):
greeneagle certification GmbH
Beim Strohhause 17
20097 Hamburg
www.greeneagle-certification.de

Prüferin und Verfasserin: Ann-Karina Wrede

Inhalt

1 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.

2 Adresse des Antragstellers

Antragstellerin der Auditierung und Zertifizierung gemäß DSAVO ist die

REISSWOLF Systems GmbH
Im Hegen 13
22113 Oststeinbek

als Hersteller des IT-Produkts REISSWOLF f.i.t. und als IT-Dienstleister.

3 Adresse der Sachverständigen Prüfstelle

Sachverständige Prüfstelle gemäß DSAVO ist die

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

unter der Leitung von Frau Ann-Karina Wrede (Recht/Technik), Legal und Technical Expert.

4 Kombiverfahren ULD und EuroPriSe

Beim vorliegenden Verfahren handelt es sich um ein Kombiverfahren von ULD und EuroPriSe, wobei das führende Verfahren das ULD-Verfahren ist.

5 Kurzbezeichnung

Auditiert wurde das Produkt REISSWOLF f.i.t. Version 1.5, ein webbasiertes Archivierungssystem zur Datenspeicherung und zum Datenzugriff.

6 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.

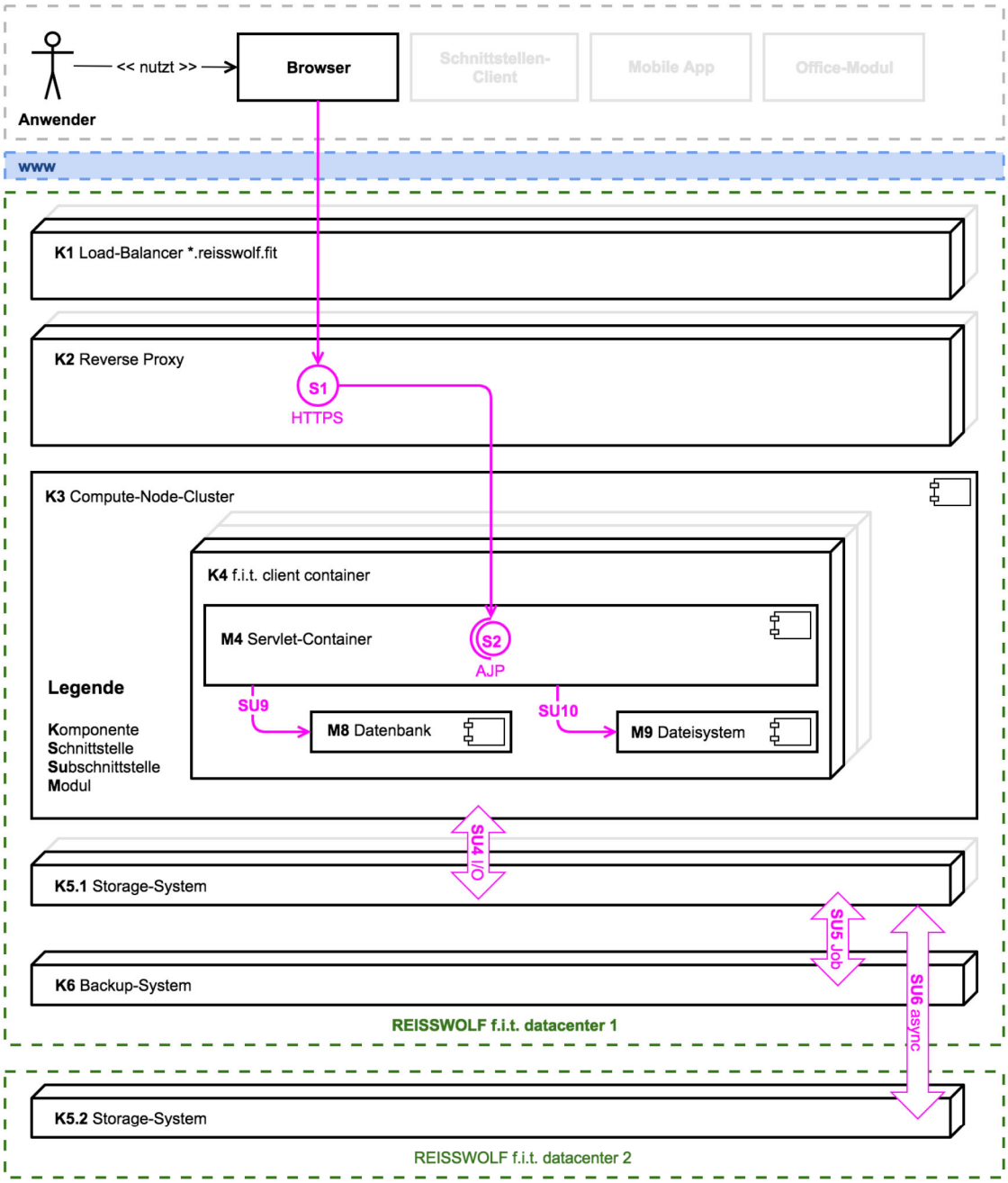
7 Zweck und Einsatzbereich

Das Produkt ist für den Einsatz bei Unternehmen (KMU), Organisationen oder öffentlichen Stellen konzipiert, unabhängig vom Land der Nutzung.
REISSWOLF f.i.t (RW f.i.t.) kommt dabei im Verantwortungsbereich des jeweiligen Anwenders zur Einsatz; d.h., es bietet den Zugang zu einer abstrahierten IT-Infrastruktur innerhalb der eigenen Organisation in einer abgeschotteten Systemumgebung.

Es ist daher auch für den Einsatz bei öffentlichen Stellen des Landes Schleswig-Holstein geeignet.

8 Modellierung des Datenflusses

Der Datenfluss von REISSWOLF f.i.t. lässt sich wie folgt darstellen:



9 Version des Anforderungskataloges

Der Prüfung lag der Anforderungskatalogs in der Version 2.0[1] des ULD und die EuroPriSe Criteria von November 2011 zugrunde.

10 Angewandte Evaluationsmethoden

Als Prüf- oder Evaluationsmethoden[2] kommen die folgenden in Betracht:

- Interviews und Befragungen
- Beobachtungen, z. B. Beobachtung von Aktivitäten und Arbeitsabläufen, Begehung, Einsicht in Konfigurationen usw.
- Durchsicht und Prüfung von Unterlagen und Dokumenten, z. B Richtlinien, Anweisungen, Verträge, Protokolle usw.

Im vorliegenden Prüfverfahren wurden sämtliche Methoden angewandt. Es wurden Interviews mit den zuständigen Mitarbeitern durchgeführt. Darüber hinaus fanden eine Vor-Ort-Besichtigung am Standort der Antragstellerin und umfangreiche Dokumentenprüfungen statt. Die Vor-Ort-Besichtigung ermöglichte sowohl die Beobachtung von Aktivitäten und Arbeitsabläufen auf Seiten der Antragstellerin als auch die Einsichtnahme in Konfigurationen.

11 Beschreibung, wie das Produkt den Datenschutz fördert

Die Förderung des Datenschutzes erfolgt auf folgende Weise:

- Der Auslieferungszustand des Programms enthält Einstellungen die ein hohes Sicherheitsniveau erzwingen. 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 im Sinne der Intervenierbarkeit 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.

[1] Anforderungskatalog v 2.0 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH mit Stand 18.11.2014.
[2] Vgl. DIN EN ISO 19011:2011-12, Punkt 6.4.6.

12 Zusammenfassung der Prüfergebnisse

12.1 Umsetzung von rechtlichen Anforderungen

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

Die Anforderungen an die Datenverarbeitung im Rahmen von Verträgen zur Auftragsdatenverarbeitung sind erfüllt.

12.2 Datensparsamkeit

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.

12.3 Datensicherheit

Im Hinblick auf die Datensicherheit sind umfangreiche Maßnahmen getroffen worden, die im 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+.
  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.

12.4 Beachtung der Betroffenenrechte

Die Beachtung der Betroffenenrechte liegt maßgeblich bei den Kunden als verantwortliche Stellen. Der Kunde wird über das Benutzerhandbuch und die dort befindlichen Datenschutzhinweise darauf hingewiesen, dass unter Umständen die Einholung von Einwilligungserklärungen und/ oder Schweigepflichtenbindungserklärungen erforderlich ist.

Die einzelnen Mitarbeiter können darüber hinaus im REISSWOLF f.i.t. ihre Rechte weitestgehend selbst wahrnehmen: Sie können ihre Daten über ihr eigenes Profil selbst ändern, berichtigen oder auch löschen. Das Löschen oder die Veränderung des Benutzernamens kann über den Kunden-Administrator vorgenommen werden, da dies wesentlich für die Anmeldung am REISSWOLF f.i.t. ist.
Darüber hinaus ist für den einzelnen Nutzer jederzeit transparent, welche Daten an welcher Stelle von ihm im REISSWOLF f.i.t. verarbeitet werden. Die Dokumente werden mit Metadaten versehen, die die Benutzer einsehen können. Dies ist zur Wahrung der Integrität und der Nachvollziehbarkeit erforderlich.
Sollten einzelne Dokumente endgültig gelöscht werden sollen, kann dies über einen Workflow beim Administrator des Kunden eingeleitet werden.

Die Betroffenenrechte werden folglich beachtet.

12.5 Datenschutzrechtliche Bewertung im Überblick

Folgende Bewertungen der Datenverarbeitung sind möglich:
- vorbildlich,
- adäquat,
- unzureichend,
- nicht einschlägig.

Dabei ist eine technische Umsetzung einer organisatorischen grundsätzlich vorzuziehen, wobei etwaige Defizite (unzureichende Umsetzung) durch eine Gesamtbewertung ausgeglichen werden kann. Die verwendeten Nummerierungen richten sich nach dem zugrundeliegenden Prüfschema bzw. der Gliederung dieses Gutachtens.

12.5.1 Primärdaten

Anforderung nach Katalog oder sonstigen Rechtsnorme	Bewertung	Kommentare
Allgemeines Anforderungsprofil		
Komplex 1:		
1.1 Verfügbarkeit, Integrität, Vertraulichkeit	vorbildlich	

1.2	Nicht Verkettbarkeit	vorbildlich	
1.3	Transparenz und Produktbeschreibung	vorbildlich	
1.4	Intervenierbarkeit	adäquat	
1.5	Frühzeitiges Löschen, Anonymisieren oder Pseudonymisieren	vorbildlich	
1.6	Anpassung des IT-Produktes	adäquat	
1.7	Privacy by Default	vorbildlich	
1.8	Sonstige Anforderungen	Nicht einschlägig	
Komplex 2:			
2.1	***Datenart 1 - Nutzerdaten***		
2.1.1	Ermächtigungsgrundlage		Im Verantwortungsbereich des Kunden
2.1.2	Gesetzliche Ermächtigung	adäquat	
2.1.3	Einwilligung des Betroffenen	adäquat	
2.1.4	Vorschriften über die Übermittlung	adäquat	
2.1.5	Löschung nach Wegfall des Erfordernisses	adäquat	
2.1.6	Einhaltung allgemeiner datenschutzrechtlicher Grundsätze und Pflichten		
2.1.6.1	Datensparsamkeit	adäquat	
2.1.6.2	Zweckbindung und Zweckänderung	vorbildlich	
2.1.6.3	Erleichterung der Umsetzung des Trennungsgebotes	adäquat	
2.1.6.4	Gewährleistung der Datensicherheit	vorbildlich	
2.1.7	Datenverarbeitung im Auftrag	vorbildlich	Bereits inkl. Anpassung auf DSGVO
2.1.8	Voraussetzung besonderer technischer Verfahren		
2.1.8.1	Trennung der Verantwortlichkeiten	adäquat	
2.1.8.2	Veröffentlichung im Internet	Nicht einschlägig	
2.1.9	Sonstige Anforderungen		
2.1.9.1	Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens	vorbildlich	
2.2	***Datenart 2 - Dokumente***		
2.2.1	Ermächtigungsgrundlage		Im Verantwortungsbereich des Kunden
2.2.1.1	Gesetzliche Ermächtigung	adäquat	
2.2.1.2	Vorschriften über die Datenerhebung und Übermittlung		Im Verantwortungsbereich des Kunden
2.2.2	Löschung nach Wegfall des Erfordernis	adäquat	Im Verantwortungsbereich des Kunden
2.2.3	Einhaltung allgemeiner datenschutzrechtlicher Grundsätze und Pflichten	adäquat	
2.2.4	Gewährleistung der Datensicherheit	vorbildlich	Bereits inkl. Anpassung auf DSGVO
2.2.5	Datenverarbeitung im Auftrag	vorbildlich	
2.2.6	Voraussetzung besonderer technischer Verfahren		
2.2.6.1	Trennung der Verantwortlichkeiten	adäquat	

2.2.6.2	Veröffentlichung im Internet	Nicht einschlägig	
2.2.6.3	Erleichterung bzw. Unterstützung von Pseudonymität	vorbildlich	
Komplex 3:			
3.1	Einzelne technisch-organisatorische Maßnahmen		
3.1.1	Physikalische Sicherung	vorbildlich	
3.1.2	Authentisierung	vorbildlich	
3.1.3	Autorisierung	vorbildlich	
3.1.4	Protokollierung	adäquat	
3.1.5	Verschlüsselung und Signatur	vorbildlich	
3.1.6	Pseudonymisieren	vorbildlich	
3.1.7	Anonymisieren	Nicht einschlägig	
3.2	Allgemeine Pflichten		
3.2.1	Technisch-organisatorische Maßnahmen		
3.2.2	Verfügbarkeit	vorbildlich	
3.2.3	Integrität	vorbildlich	
3.2.4	Vertraulichkeit	vorbildlich	
3.2.5	Nicht-Verkettbarkeit	vorbildlich	
3.2.6	Transparenz	adäquat	
3.2.7	Intervenierbarkeit	vorbildlich	
3.2.8	Protokollierung von Datenverarbeitungsvorgängen	adäquat	
3.2.9	Test und Freigabe	adäquat	Zertifizierung ISO 27001:2013
3.2.10	Sicherheitsrichtlinie	adäquat	Zertifizierung ISO 27001:2013
3.2.11	Risikoanalyse	adäquat	Zertifizierung ISO 27001:2013
3.2.12	Inventarisierung (Hardware, Software, Daten und Datenträger)	adäquat	Zertifizierung ISO 27001:2013
3.2.13	Datenträger-Management	adäquat	Zertifizierung ISO 27001:2013
3.2.14	Datenschutz- und Informationssicherheitsbeauftragter	adäquat	Zertifizierung ISO 27001:2013
3.2.15	Interne Audits	adäquat	Zertifizierung ISO 27001:2013
3.2.16	Vorfallsmanagement	adäquat	Zertifizierung ISO 27001:2013
3.2.17	Erleichterung der Vorabkontrolle	adäquat	
3.2.18	Erleichterung bei der Erstellung des Verfahrensverzeichnis	vorbildlich	
3.2.19	Benachrichtigungspflicht bei unrechtmäßiger Kenntniserlangung von Daten	vorbildlich	
3.2.20	Unterstützung der Tätigkeit des Datenschutzbeauftragten	adäquat	
3.3	Spezifische Pflichten	adäquat/ vorbildlich	
3.4	Pflichten nach Datenschutzverordnung	adäquat	
3.5	Anforderungen an den Betrieb bei Auftragsdaten-verarbe tung	adäquat	
3.6	Sonstige Anforderungen	Nicht einschlägig	
Komplex 4:			
4.1	Aufklärung und Benachrichtigung	vorbildlich	
4.2	Benachrichtigung des Betroffenen bei unrechtmäßiger	vorbildlich	

	Kenntniserlangung		
4.3	Auskunft	adäquat	
4.4	Berichtigung, Löschung und Sperrung	vorbildlich	
4.5	Sonstige Anforderungen	Nicht einschlägig	

12.5.2 Sekundärdaten

Anforderung nach Katalog oder sonstigen Rechtsnormen	Bewertung	Kommentare
1. Protokolldaten (Mitarbeiter des Kunden)		
1.1. Komplex 1: Grundsätze der Datenverwendung		
1.1.1 Datenvermeidung und Datensparsamkeit	adäquat	
1.1.2 Nicht-Verkettbarkeit und Transparenz	adäquat	
1.2 Komplex 2: Rechtmäßigkeit		
1.2.1 Zulässigkeit	adäquat	
1.2.2 Zweckbindung	adäquat	
1.2.3 Aufbewahrung und Löschung	adäquat	
1.3 Komplex 3: Technische und organisatorische Maßnahmen	vorbildlich	
1.4 Komplex 4: Betroffenenrechte	adäquat	
2. Accountdaten (Downloadverlauf, Workflow, Papierkorb)		
2.1. Komplex 1: Grundsätze der Datenverwendung		
2.1.1 Datenvermeidung und Datensparsamkeit	adäquat	
2.1.2 Nicht-Verkettbarkeit und Transparenz	adäquat	
2.2 Komplex 2: Rechtmäßigkeit		
2.2.1 Zulässigkeit	adäquat	
2.2.2 Zweckbindung	adäquat	
2.2.3 Aufbewahrung und Löschung	adäquat	
2.3 Komplex 3: Technische und organisatorische Maßnahmen	vorbildlich	
2.4 Komplex 4: Betroffenenrechte	adäquat	
3. Ticketsystem		
3.1 Komplex 1: Grundsätze der Datenverwendung		
3.1.1 Datenvermeidung und Datensparsamkeit	adäquat	
3.1.2 Nicht-Verkettbarkeit und Transparenz	adäquat	
3.2 Komplex 2: Rechtmäßigkeit		
3.2.1 Zulässigkeit	adäquat	
3.2.2 Zweckbindung	adäquat	
3.2.3 Aufbewahrung und Löschung	adäquat	Dokumente befinden sich in Überarbeitung
3.3 Komplex 3: Technische und organisatorische Maßnahmen	adäquat	
3.4 Komplex 4: Betroffenenrechte	adäquat	
4. Protokolldaten (Mitarbeiter von REISSWOLF)		
4.1 Komplex 1: Grundsätze der Datenverwendung		
4.1.1 Datenvermeidung und Datensparsamkeit	adäquat	
4.1.2 Nicht-Verkettbarkeit und Transparenz	adäquat	
4.2 Komplex 2: Rechtmäßigkeit		
4.2.1 Zulässigkeit	adäquat	
4.2.2 Zweckbindung	adäquat	

4.2.3	Aufbewahrung und Löschung	adäquat	
4.3	Komplex 3: Technische und organisatorische Maß-nahmen	adäquat	
4.4	Komplex 4: Betroffenenrechte	adäquat	

13 Votum

Hiermit bestätige ich, dass das Produkt REISSWOLF f.i.t. und der dazugehörende IT-Service zum Zeitpunkt der Begutachtung den Rechtsvorschriften über den Datenschutz und der Datensicherheit entsprechen. Die ausführliche Analyse liegt anbei.

[redacted]

Digital unterschrieben von Ann-Karina Wrede
DN: cn=Ann-Karina Wrede, email=awrede@greeneagle-certification.de, c=DE
Datum: 2018.05.22 09:12:52 +02'00'

Hamburg, 22.05.2018

Ann-Karina Wrede
Rechtsanwältin, Master of Arts in IT-Managements
Leiterin der beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannten Sachverständigen Prüfstelle für IT-Produkte (Recht/Technik)
EuroPriSe Legal and Technical Expert