Kurzgutachten zur Erteilung eines Datenschutzgütesiegels für „DRACOON“

im Auftrag der DRACOON GmbH

datenschutz cert GmbH

17.01.2018

Inhaltsverzeichnis

1. Vorbemerkung

Mit diesem Kurzgutachten werden die Ergebnisse der datenschutzrechtlichen und IT-sicherheitstechnischen Auditierung des „DRACOON“ in der Version 4 (Unterversion 4.5.0) gemäß der Datenschutzgütesiegelverordnung (DSGSVO) Schleswig-Holsteins[1] zusammengefasst. Die Auditierung des IT-basierenden Services bezog sich dabei auf den Funktionsstand im Januar 2018.

DRACOON ist der Nachfolger des ebenfalls zertifizierten Secure Data Space (SDS).

2. Zeitraum der Prüfung

Die Begutachtung erfolgte vom 06.06.2017 bis 17.01.2018 und beinhaltete neben der konzeptionellen Analyse der zur Verfügung gestellten Unterlagen Funktionstests anhand von Testzugängen. Hierbei sind auch die Verschlüsselungsmechanismen überprüft worden.

3. Antragstellerin

Antragstellerin ist die

DRACOON GmbH

Galgenbergstrasse 2a

93053 Regensburg, Bundesrepublik Deutschland

als Anbieter des „DRACOON“. Ansprechpartner ist Herr Dr. Florian Scheurer, Chief Technical Officer der DRACOON GmbH.

4. Sachverständiger/Prüfstelle

Sachverständige Prüfstelle ist die

datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen

unter der Leitung von Herrn Dr. Sönke Maseberg (Technik) und Frau Irene Karper (Recht). Ansprechpartner für diese Prüfung sind:

Bereich „Recht“:	Bereich „Technik“:
Frau Dr. Irene Karper datenschutz cert GmbH Konsul-Smidt-Str. 88a 28217 Bremen	Herr Alexey Testsov datenschutz cert GmbH Konsul-Smidt-Str. 88a 28217 Bremen.

5. Kurzbezeichnung des IT-Produkts

DRACOON in der Version 4 (Unterversion 4.5.0), Funktionsstand Januar 2018.

[1] Landesverordnung über ein Datenschutzgütesiegel v. 30.11.2013, GVOBl. Schl.-H. 2013, S.536ff. Konkretisiert wird die DSGSVO durch den Anforderungskatalog des ULD, der zum Zeitpunkt des Audits in der Version 2 vorlag. Die Kriterien sind abrufbar unter https://www.datenschutzzentrum.de/uploads/guetesiegel/guetesiegel-anforderungskatalog.pdf. Stand dieser und weiterer hier zitierter Webseiten ist Oktober 2017.

6. Beschreibung des IT-Produkts

DRACOON ist ein webbasierender, virtueller Datenraum, in welchem Daten hochgeladen, gespeichert, verwaltet und ausgetauscht werden können. DRACOON ist eine typische Cloud-Dienstleistung.

DRACOON wird von der DRACOON GmbH vertrieben und als *Software as a Service* (SaaS) im Auftrag für den Anwender am Standort in Regensburg entwickelt, gepflegt und in einem Rechenzentrum in Nürnberg betrieben. DRACOON wird in folgenden Varianten angeboten:

- DRACOON Online
- DRACOON Branded Cloud (ehemals „Dedicated“)
- DRACOON for Windows/Linux, Enterprise, OEM (ehemals “Virtual Appliance).

DRACOON Online ist die Standardausführung. Sie wird von der DRACOON GmbH als SaaS angeboten. *Branded Cloud* entspricht der Standardausführung. Allerdings erhält der Anwender die Möglichkeit, DRACOON auf seine Bedürfnisse und das Corporate Design zu branden sowie eine Anmeldung über Active Directorys zu erhalten. *DRACOON für Windows/Linux, Enterprise, OEM* ist dagegen ein Softwarepaket, das einerseits vom Anwender in seiner eigenen Umgebung installiert und gehostet werden, andererseits als SaaS beauftragt werden kann.

7. Tools, die zur Herstellung des Produkts verwendet wurden

Keine Relevanten.

8. Zweck und Einsatzbereich

DRACOON ist für den gewerblichen B2B- Einsatz konzipiert. **Anwender** sind Unternehmen, Organisationen oder öffentliche Stellen. DRACOON kommt dabei im Verantwortungsbereich des lizenzierten Anwenders zum Einsatz, so dass es sich um eine Private-Cloud-Dienstleistung handelt. Der Anwender kann als Lizenznehmer aus den genannten Varianten wählen.

Anbieter ist die DRACOON GmbH (ehemals SSP Europe GmbH). Das Informationsmanagementsystem der DRACOON GmbH ist gemäß ISO/IEC 27001 zertifiziert.

Im Unterauftrag der DRACOON GmbH ist die ANEXIA Internetdienstleistungs GmbH, Feldkirchnerstraße 140, 9020 Klagenfurt, Österreich, für die Bereitstellung der VM-Infrastruktur von DRACOON tätig. Die Tätigkeit erfolgt dabei durch Wartung und Austausch von Hardware und Software im Rechenzentrum in Nürnberg. Die ANEXIA Internetdienstleistungs GmbH ist gemäß ISO/IEC 27001 zertifiziert.

Kundenverträge sowie Verträge mit den Dienstleistern der DRACOON entsprechen den Anforderungen an eine Auftragsverarbeitung und unterstützen so die Anforderungen der Datenschutzaufsichtsbehörden zum Cloud Computing[2].

[2] Z.B. gemäß der *„Orientierungshilfe – Cloud Computing“* der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder oder gemäß des Working Paper No. 196 der Artikel-29-Datenschutzgruppe (*„Opinion 05/2012 on Cloud Computing“).*

Ferner wird ein SMS-Gateway und das Kommunikationsnetz der Deutschen Telekom AG genutzt. Der gehört aber nicht zu dem Zertifizierungsgegenstand.

DRACOON ist im Internet unter https://dracoon.team/ erreichbar.

Abb. 1: Login DRACOON

Der Anwender definiert den Anwendungsbereich und welche Benutzer Zugriff auf DRACOON, die Data Rooms und die Dateien bekommen. Zugriffsberechtigt können z.B. interne Bereiche oder einzelne Mitarbeiter sein aber auch andere Unternehmen. Die Organisationsstruktur kann über die Data Rooms abgebildet werden (z.B. Fachbereich). DRACOON stellt hierfür ein detailliert abstufbares Berechtigungskonzept zur Verfügung. Die Funktionen von DRACOON sind für den Anwender im Benutzerhandbuch transparent dokumentiert. Im **DRACOON** gibt es folgende Funktionen:

- --- Ablaufdatum für Files, Benutzeraccounts und Downloadlinks
- --- Kommentarfunktion für Dateien
- --- Sortierung nach User, Datum, Typ, Größe, Name
- --- Up- und Downloads als Zip-Archiv
- --- Dateiaustausch als öffentliche Downloadlinks/Quicklinks (optional passwortgeschützt, zeitlich limitiert)
- --- Verschlüsselte Ablage aller Nutzdaten sowie aller temporären Kennwörter z.B. für Accounts oder Datei-Freigaben; dadurch ist kein Zugriff des Providers auf die Daten des Anwenders möglich

- --- Dateien werden nach Upload automatisch vom Anti-Viren-Scanner überprüft (sofern Dateien nicht verschlüsselt sind). Ist eine Datei infiziert, wird der Versuch einer Desinfektion unternommen. Gelingt dies nicht, so wird die Datei auf die Endung „.virus“ umbenannt und der Zugriff wird gesperrt. Die betroffenen Dateien werden nicht automatisch, sondern nur manuell vom System entfernt. Ein Umbenennen ist nur in Zusammenarbeit mit dem Betreiber möglich.
- --- Zugriff mittels Benutzerkonten per E-Mail-Adresse / Kennwort als Standard
- --- Einbindung der Data Rooms in das IT-Netzwerk des Anwenders möglich
- --- Einfache Einbindung als Laufwerk (PC, MAC, LINUX)
- --- Konfigurierbare, temporäre Upload-Konten für den zeitlich und volumentechnisch beschränkten Zugriff durch Drittbenutzer / Geschäftspartner des Anwenders zum Hochladen von Dateien
- --- Sämtliche Events, wie IPs, Zugriffe, Änderungen, Uploads etc. werden optional revisionssicher protokolliert
- --- Administration und Dateiaustausch über die Webapplikation (WebGUI)
- --- Mehrsprachiges Interface: Deutsch, Englisch, Spanisch (Sprachen sind erweiterbar)
- --- Backup kompletter Data Rooms manuell durch Data Room Admins oder Data Space Admins möglich oder automatisiert (über einen sogenannten Backup-Agenten)
- --- Verschlüsselung von Data Rooms mittels clientseitiger Verschlüsselung.

DRACOON ermöglicht die Klassifizierung von Vertraulichkeits-Stufen beim Upload in

- --- öffentlich
- --- nur für interne Nutzung
- --- vertraulich und
- --- streng vertraulich.

Der Benutzer kann die Klassifizierung innerhalb seines Data Rooms bei der Verarbeitung der gewünschten Datei einfach auswählen.

Zusätzlich zu den Grundfunktionalitäten des DRACOON Online bietet **DRACOON Branded Cloud** nachfolgende Besonderheiten:

- --- Eine dediziert für den Anbieter bereitgestellte Storage-Umgebung
- --- Ein dediziertes Kennwort für die Verschlüsselung der Storage Umgebung
- --- Ein Branding der Umgebung nach Vorgaben des Anwenders
- --- Es sind Active Directory-Anmeldungen möglich
- --- Der Zugriff aus dem Internet kann über eine beliebige Adresse im Rahmen der Domains des Anwenders über ein vorhandenes oder durch die DRACOON GmbH zur Verfügung gestelltes SSL Zertifikat erfolgen.

Zusätzlich DRACOON Online und DRACOON Branded Cloud bietet **DRACOON for Windows/Linux, Enterprise, OEM**:

--- Nutzung beim Anwender als Inhouse-Lösung

--- Anbindung an den vom Anwender bereitgestellten Storage nach Vorgaben der DRACOON GmbH

--- Nutzung im Housing Betrieb oder im Data Center des Anwenders.

8.1 Login und Authentisierung

Der Benutzer verbindet sich per SSL zum Frontend und authentisiert sich mit Benutzername und Passwort. Bei der erstmaligen Anmeldung zu DRACOON muss das Passwort geändert werden. Es muss mindestens 8 Zeichen besitzen und aus Buchstaben und Ziffern bestehen, die automatisiert gegengeprüft werden. Der Anwender wird in einem Merkblatt zum Datenschutz darauf hingewiesen, den Passwortschutz zu nutzen. Das Merkblatt ist Vertragsbestandteil und innerhalb des Accounts von DRACOON abrufbar. Es ist allerdings möglich, dass auf Wunsch der Anwender des DRACOON Branded Cloud sowie des DRACOON for Windows/Linux, Enterprise, OEM eine andere Passwortkonvention implementiert wird. Bei Falscheingaben des Passwortes wird der Account gesperrt. Die Benutzernamen werden im Klartext in der Datenbank gespeichert, die Passwörter werden verschlüsselt und als Hash abgelegt. DRACOON verwendet einen aus Sicht der Auditoren gut konzipierten Authentisierungsmechanismus. Bei der Standard-Authentisierung wird das Passwort mittels bcrypt/Salting in der Datenbank abgelegt. Das Rücksetzen des Passwortes geschieht über die E-Mail-Adresse, an welche ein auf 24h-Gültigkeit begrenzter Link gesendet wird. Hier kann der Benutzer sein Passwort selbst zurücksetzen. Ab der Version 3.3 wurde es Anwendern ermöglicht, ihre eigene E-Mail-Adresse, die für den Login und für den Empfang von Meldungen genutzt wird, durch eine andere zu ersetzen. Dies gilt nicht für den Fall, dass eine Active-Directory-Anbindung genutzt wird; in diesem Fall muss die Änderung über das AD erfolgen. Bei den Varianten DRACOON Branded Cloud und DRACOON Windows/Linus, Experience OEM ist auf Wunsch des Anwenders eine Authentifizierung durch die Anbindung an ein oder mehrere Active Directory möglich. Der Benutzer meldet sich dann mit seinem AD-Benutzernamen und dem -Passwort an. Der Authentisierungsprozess bei Standardinstallation, bei dem sich Benutzer mit den in der Datenbank gespeicherten Login-Daten anmelden können, bleibt ebenfalls möglich. Somit ist sichergestellt, dass auch externe Benutzer, die kein Konto im AD besitzen, DRACOON nutzen können. Alternativ kann die Authentisierung gegen einen Radius Server per Token erfolgen. Der Benutzer meldet sich mit seinem Benutzernamen, einer PIN und einem durch den Token generierten Einmalpasswort an. Die Anmeldung mittels der in der Datenbank gespeicherten Login-Daten wird in diesem Fall unterbunden. Nach der Anmeldung gelangt der Benutzer auf ein Dashboard als Startseite:

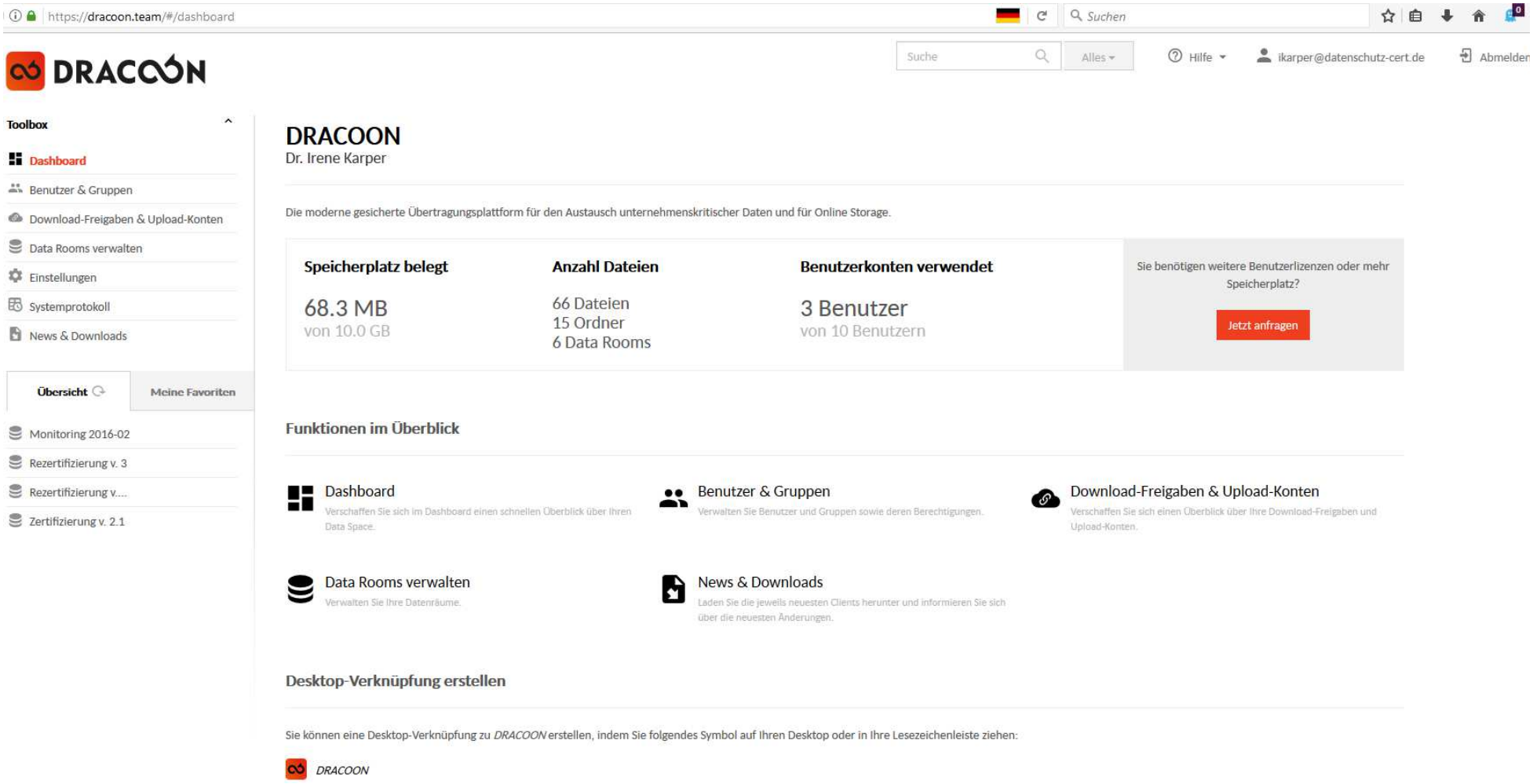


Abbildung 1: Dashboard

8.2 Verschlüsselung

Die Datenübertragung zwischen Server und Client erfolgt mittels SSL Verbindung und einem zum Auditzeitpunkt bis Oktober 2018 gültigen Zertifikat. Die DRACOON GmbH bietet auf Wunsch des Anwenders Verschlüsselungsgrade bis zu 256 Bit an, sofern die eingesetzten Webbrowser und Betriebssysteme dies unterstützen. Die Datenbank selbst ist nicht verschlüsselt. Daten werden aber auf einem LUKS-verschlüsselten Datenträger innerhalb des gesicherten Rechenzentrums gespeichert, so dass hierdurch ein zusätzlicher Diebstahlschutz gewährleistet wird. Optional können Daten vor Übertragung in den Data Room clientseitig verschlüsselt werden. Bei einer Verschlüsselung wird der gesamte Data Room verschlüsselt, was nur im leeren Zustand möglich ist. Jeder Benutzer wird bei erstmaliger Nutzung eines Spaces mit aktiviertem „Triple-Crypt“ aufgefordert, ein Verschlüsselungs-Passwort zu wählen, aus dem ein Schlüsselpaar (RSA-2048) generiert wird. Dieses Schlüsselpaar kommt in allen verschlüsselten Data Rooms dieses Data Spaces zum Einsatz. Für jedes Dokument, das nun hier abgelegt wird, wird ein zufälliger symmetrischer Schlüssel (AES256) generiert, mit dem das Dokument unter Verwendung des Galois Counter Mode (GCM) verschlüsselt wird. Dieser symmetrische Schlüssel wird anschließend mit dem öffentlichen Schlüssel aller für diesen Data Room berechtigten Benutzer verschlüsselt und zusammen mit den verschlüsselten Daten in der Datenbank abgelegt. Somit können alle Benutzer, die für einen Data Room Leseberechtigung haben, alle Daten in diesem Data Room lesen, auch wenn diese verschlüsselt sind. Sollen diese nur für einen Benutzer lesbar sein, ist es möglich einzelne Sub-Rooms anzulegen, für die nur einzelne Benutzer Leseberechtigung haben. Zum Lesen einer verschlüsselten Datei wird der Benutzer aufgefordert, sein Verschlüsselungs-Kennwort einzugeben, womit der private Schlüssel freigegeben wird, um den symmetrischen Schlüssel entschlüsseln und verwenden zu können. Der Ver- und Entschlüsselungsvorgang wird per JAVA Script oder Java Applet im Browser des DRACOON Benutzers am Client durchgeführt. Die Keys werden aus der Datenbank angefordert und im Speicher des Clients vorgehalten. Über diese Kombination und dieses Verfahren ist bei durch den DRACOON Benutzer aktivierten, clientseitigen Verschlüsselung zu keinem Zeitpunkt eine Datei unverschlüsselt auf den DRACOON Backend-Systemen vorhanden und somit auch durch keinen Administrator der DRACOON GmbH einsehbar, auch nicht auf dem Transportweg.

Mit der Version 3.9 wurden die Verschlüsselungsmöglichkeiten erweitert. Bei Upload-Accounts wird dem externen Benutzer der Public Key des Erstellers ausgeliefert. Somit ist eine Verschlüsselung der Datei einfach für externe Benutzer möglich. Dabei wird nicht preisgegeben, welche und wie viele weitere Benutzer Berechtigungen auf dem Datenraum besitzen. Der bereitgestellte öffentliche Schlüssel trägt keinerlei Identitätsinformationen des Eigentümers, es handelt sich also ausdrücklich nicht um ein Zertifikat. Für Download-Links wird bei Erstellung ein eigenes Schlüsselpaar erzeugt, für das auf die übliche Art und Weise eine Kopie des Dateischlüssels bereitgestellt wird. Das Freigabepasswort dieses Links schützt auf kryptographischer Basis den neu erzeugten Private Key und schafft somit ein Analogon zu dem Verschlüsselungspasswort des registrierten Benutzers. Der externe Benutzer muss dieses Passwort bei der Nutzung des Freigabelinks eingeben, die Weboberfläche entschlüsselt mit den bereits intern genutzten Funktionen erst den privaten Schlüssel und anschließend die Datei (über die Nutzung des individuell verschlüsselten Dateischlüssels („FileKey“). Auf diese Weise ist sichergestellt, dass ohne

Kenntnis des Passworts auch der Plattformbetreiber keinen Einblick in die über Freigabelinks geteilten Dateien aus verschlüsselten Datenräumen nehmen kann.

DRACOON bietet die Möglichkeit für den Notfall Rescue Keys einzurichten. Wenn Triple-Crypt aktiviert wird, hat der Data Space-Admin die Möglichkeit, einen Data Space Rescue Key einzurichten. Wird ein neuer Data Room angelegt, so hat der Data Room-Admin die Möglichkeit zu entscheiden, ob für diesen Data Room der Data Space Rescue Key als Notfallschlüssel verwendet werden soll, ob ein eigener Data Room Rescue Key erzeugt und verwendet werden soll oder ob es keinen Rescue Key für diesen Data Room geben soll. Die Rescue Keys sind technisch gesehen Schlüsselpaare für asymmetrische Verschlüsselung und unterscheiden sich nicht von den Nutzer-Schlüsselpaaren. Der private Schlüssel ist über ein langes und komplexes Passwort gesichert, welches von der entsprechenden Rolle (Data Space-Admin oder Data Room-Admin) durch organisatorische Maßnahmen geeignet geschützt wird. Sämtliche symmetrischen File-Keys eines Data Rooms werden, wenn ein Rescue-Key verwendet wird, mit allen öffentlichen Schlüsseln der berechtigten Nutzer und des entsprechenden Rescue-Keys verschlüsselt und in der Datenbank abgelegt. Bei Verwendung eines Data Space Rescue Keys ist durch das Berechtigungskonzept sichergestellt, dass ein Data Space Admin auch bei Kenntnis des Data Space Rescue Keys nur auf Daten zugreifen kann, die für ihn durch den jeweiligen Data Room Admin freigegeben worden sind. Die Rescue Keys dienen als Sicherheitsanker, für den Fall, dass alle Benutzer eines Data Rooms ihre Verschlüsselungs-Passwörter vergessen haben. Mit Hilfe des Rescue Keys sind die Daten dann noch entschlüsselbar. Wird kein Rescue-Key verwendet, sind die Daten nicht mehr zu entschlüsseln.

8.3 Datenlöschung, Datenminimierung, Übertragbarkeit

Löschvorgänge werden zwischen der DRACOON GmbH und dem Anwender vertraglich geregelt. Primärdaten können vom Anwender selbst gelöscht werden oder bereits bei Erstellung mit einem Löschdatum (Ablaufdatum) versehen werden. Im letzteren Fall werden die markierten Dateien nach Ablauf der Löschfrist per cronjob vollständig gelöscht. Zugehörige Sekundärdaten wie Änderungsprotokolle bleiben bis zur Kündigung von DRACOON durch den Anwender erhalten. Logdaten, die einer Angriffserkennung dienen, werden, sofern nicht anders beauftragt, nach 7 Tagen gelöscht. Auf Wunsch des Anwenders können Logdaten länger vorgehalten und bereitgestellt werden. Hierfür ist ein gesonderter Auftrag erforderlich. Die übliche Aufbewahrungsfrist beträgt dann in der Regel drei Monate. Mit Version 3.2 wurde eine Papierkorbfunktion neu eingeführt, bei welcher der Data Room Admin eine Zeitspanne definieren kann, in der Dateien automatisiert entfernt werden. Mit der Version 3.8 können Data Space Admin beim Anlegen eines Data Rooms festlegen, welches Datenvolumen („Quota“) dort abgelegt werden darf. Ist das Volumen überschritten, ist kein Upload mehr möglich, bis Speicher freigegeben wurde. Bei Kündigung erhält der Anwender die Möglichkeit, sämtliche Daten per zip-Archiv zu exportieren.

8.4 Activity Log

Mit Version 3.9 steht für jeden Datenraum ein Activity Log bereit, dass es berechtigten Benutzern ermöglicht, Einblick in eine aggregierte Sicht auf die Modifikationen von Dateien zu nehmen (z.B. neue, modifizierte oder gelöschte Dateien). Dabei werden ausschließlich Dateioperationen gelogged, die ein Benutzer ohnehin anhand der

Metainformationen der Objekte einsehen könnte. Das Activity Log ist daher lediglich eine komfortablere Form der Aufbereitung. Zudem besteht die Möglichkeit, das Activity Log global zu deaktivieren.

8.5 Audit Log

Über ein Audit Log können Data Space Administratoren Transaktionen suchen, einsehen und nachvollziehen, die mandantenbezogen ausgeführt wurden. Das Audit Log ist systemseitig nicht veränderbar und kann nur gelöscht werden, indem eine Löschung des Mandanten erfolgt.

8.6 Komponenten

DRACOON umfasst Komponenten:

--- WebUI

--- JSON-REST-API-Schnittstelle

--- DRACOON-Server

--- Management Database.

Der Zugriff auf DRACOON erfolgt über gängige Webbrowser. DRACOON kann dabei auch über mobile devices (Smartphones, Tablets) abgerufen werden. **Apps und mobile devices sind kein Bestandteil des Audits.**

Ferner kann DRACOON über die Schnittstelle WebDAV als Laufwerk bei einem Anwender eingebunden werden. In dem Fall steht die clientseitige Verschlüsselung allerdings nicht zur Verfügung. Der Anwender wird im Datenschutzmerkblatt darauf hingewiesen, vertrauenswürdige Clients zu nutzen.

Mit den Versionen 3.4 und 3.5 wurde die Konfiguration der API-Schnittstelle zur verbesserten Integration des AD neu aufgesetzt. Der DRACOON-Server bietet weiterhin eine JSON-REST-API an, über die sämtliche Funktionalität der Software abgebildet ist. Somit ist sämtliche Funktionalität und Logik des Programmablaufes aus den Client-Anwendungen in den Server verlagert worden. Diese API stellt inzwischen die einzige Schnittstelle zu jeglichen Anwendungen dar, die an DRACOON angebunden werden. Somit gelten automatisch für alle Clients die gleichen Sicherheitsanforderungen und -mechanismen sowie sämtliche datenschutzrelevanten Komponenten. Die Clients selbst tragen nur diejenige Logik in sich, die sie für die Darstellung der bereitgestellten Informationen auf dem Bildschirm des Benutzers benötigen oder die eine Integration von DRACOON in bestehende Umgebungen, Systeme und Workflows ermöglichen – und natürlich die Funktionalität, die für die client-seitigen kryptographischen Operationen benötigt wird. Die WebUI –der Standard-Client, auf den Benutzer zurückgreifen können und der einzige Client, der von Hause aus den vollständigen Funktionsumfang bereitstellt – wird ebenfalls in der Umgebung der DRACOON GmbH gehostet. Allerdings besitzt die neue WebUI keine server-seitige Logik (wie es bei klassischen Web-Anwendungen z.B. in PHP oder JSP der Fall wäre), sondern führt die gesamte Darstellung der Oberfläche in Form von JavaScript im Browser des Clients aus. Dieser kommuniziert direkt mit der API, um die dafür benötigten Daten zu beziehen. Sämtliche weitere Schnittstellen, die nicht innerhalb des Scopes der Zertifizierung liegen, werden ebenfalls über die JSON-REST-API realisiert. Dabei wurde für die WebDAV- und SFTP-Schnittstellen ein Proxy entwickelt, die

die Kommunikation mit den entsprechenden Clients über das bereitgestellte Protokoll auf die API mappen.

DRACOON enthält folgende Schnittstellen:

- --- https-Zugriff auf das WebUI
- --- interne MySQL-Datenbankschnittstelle
- --- Java/IO Funktion zum local mount und zur Dateiablage
- --- smtp für Mailversand (Versenden von Links zum Download)
- --- API-Schnittstelle
  - --- sftp-Schnittstelle via API
  - --- WebDav Schnittstelle (zur Einbindung als Laufwerk beim Anwender) via API
  - --- Schnittstelle für Mobile Apps und Drive Letter

8.7 Berechtigung und Rollen

Berechtigungen können entsprechend der Rollen und Funktionen abgestuft und detailliert zugewiesen werden:

ROLLENKONZEPT	DATA SPACE ADMIN Zentrale Adminfunktion	DATA ROOM ADMIN Admin für Data Room	DATA ROOM USER Typischer Benutzer	LINK EMPFÄNGER Temporärer User
Festlegung globaler Systemeinstellungen	+	–	–	–
Globale Benutzerverwaltung	+	–	–	–
Anlegen von neuen Data Rooms und Zuweisung von Data Room Admins	+	–	–	–
Rechteverwaltung innerhalb der Data Rooms	–	+	–	–
Benutzerverwaltung innderhalb der Data Rooms	–	+	–	–
Verschlüsselung von Data Rooms	–	+	–	–
Hochladen, Löschen und Versenden von Dateien	+	+	+	–
Nutzen von Down- und Uploadlinks	+	+	+	+

Abbildung 2: Rollenkonzept

8.7.1 Data Space Admin

Der Data Space Admin besitzt die zentrale Administrationsfunktion des Anwender-Accounts mit einem Gesamtüberblick sowie allen Rechte auf die Data Space Rooms und Subrooms sowie die User-/Rechteverwaltung. Mit Version 4.0 erfolgte eine Unterteilung in fünf Rollen: Config Manager, Room Manager, User Manager, Group Manager sowie Log Auditor, die jeweils separat an Benutzer und Benutzergruppen vergeben werden können.

8.7.2 Data Room Admin

Der Data Room Admin ist der Administrator des jeweiligen Data Rooms, hat einen Überblick über die Benutzer, vergibt die Benutzerrechte (Upload, Löschen, Data Room Admin), kann Subrooms anlegen und bearbeitet Zuweisungen zu Data Rooms (Benutzer

hinzufügen, entfernen). Er kann gleichzeitig in verschiedenen Data Rooms / Subrooms Data Room Admin oder Data Room User sein. Mit der Version 3.0 hat jeder Data Room Admin automatisch die Möglichkeit, mit wenigen Klicks in seinen Räumen die clientseitige Verschlüsselung zu aktivieren. Seit Version 3.9 kann der Data Room Admin für jeden Benutzer individuell einen initialen Datenraum festgelegen, der dem Benutzer direkt nach dem Login anstelle des Dashboards angezeigt wird.

8.7.3 Data Room User

Der Data Room User kann in seinem Account Dateien hochladen, löschen und Downloadlinks versenden, als Favoriten markieren, suchen (je nach zugeteilten Rechten) und – je nach Anforderung beim Anwender - zugleich die Rolle eines Data Room Admin innehaben. Ferner ist es möglich, Rechte auf Datenräume unterer Hierarchieebenen zu vererben. Dies ist für eine Datenraumstruktur, die sich nun über viele Ebenen erstrecken kann, erforderlich, da die jeweils individuelle Konfiguration sämtlicher Berechtigungen aller Benutzer auf jeder Ebene eine enorme Fehlerquelle für den Benutzer darstellen kann. Mit Version 4.0 wurde die Einschränkung aufgehoben, dass Datenräume lediglich auf den beiden obersten Ebenen angelegt werden können. Dadurch können nun sämtliche Strukturen eines Unternehmens über Datenräume abgebildet werden. Es wurde zudem eine Drag&Drop-Funktion für Dateien eingeführt. Markiert man Dateien, kann man über die neue „Benachrichtigen“-Schaltfläche sehr einfach eine E-Mail erzeugen lassen, die Verweise auf die ausgewählten Dateien enthält. Dies ermöglicht den komfortablen Versand von Hinweisen an andere Benutzer.

8.7.4 Link-Empfänger und Upload Konto

Nutzer der Downloadlinks bzw. die Nutzer des Upload-Kontos müssen keinen eigenen Account bei DRACOON besitzen. Die Links bestehen aus einer zufälligen Zeichenkombination, so dass keine Rückschlüsse anhand der Nummerierung o.Ä. möglich sind. Die Freigabelinks erhalten 32 Stellen (A-Z, a-z, 0-9). Es gibt 62^{32} (Größenordnung: 10^{57}) unterschiedliche Links, die darüber hinaus zusätzlich (wie gehabt) mit einem Passwort geschützt werden können. Es ist einfach, unterschiedliche Freigabelinks (mit unterschiedlichen Passwörtern und Ablaufdaten) für die gleiche Datei anzulegen. Somit erhalten unterschiedliche Benutzer unterschiedliche Links und müssen nicht das gleiche Passwort erfahren oder wiederverwenden. Die maximale Anzahl an Downloads eines Freigabelinks kann festgelegt, z.B. auf die maximale Anzahl von *1*. Damit werden die Daten nach dem ersten Aufruf unzugänglich. Sollte der Download nicht mehr möglich sein werden, so kann man feststellen, dass die Informationen unberechtigt heruntergeladen wurden und somit als kompromittiert gelten müssen.

8.7.5 Optional: Freigabe des Passwortes per SMS

Wenn ein Freigabelink passwortgeschützt erzeugt wird, dann erhält der Nutzer seit Version 4.1 die Option, das gewählte Passwort optional per SMS versenden zu lassen. Dazu muss die Mobilfunknummer des Empfängers bereitgestellt werden. Der Anwender muss diese Funktion in den Systemeinstellungen erst aktiv freischalten. Dieses Feature wurde ergänzt, damit das Geheimnis geteilt wird: Einerseits wird in der E-Mail weiterhin der Link verschickt, anderseits wird das Passwort dann über einen zweiten Kanal als SMS übertragen. Diese Funktion ist nur bei unverschlüsselten Dateien möglich; denn bei der Freigabe von verschlüsselten Dateien darf auch der Server keine Kenntnis des Passworts

erlangen, da ansonsten das Ende-zu-Ende-Prinzip verletzt wäre. Wird diese Funktion genutzt, erzeugt der Server eine Kurzmitteilung, die neben einem einfachen Hinweis das Passwort enthält und sendet diese an die durch den Benutzer eingegebene Mobilfunknummer. Die einzigen bereitgestellten Informationen sind eine MSISDN sowie das gewählte Passwort –in diesem Fall jedoch ohne zugehörigen zufälligen Link. D.h. auch durch Kenntnis der Kurzmitteilung ist der Download der Datei nicht möglich; man ist auf den über einen anderen Kanal (i.d.R. E-Mail) übermittelten zufälligen Link angewiesen (ca. 192 Bit Entropie). Für den SMS-Versand wird ein Gateway der Deutschen Telekom AG eingesetzt. Die Einlieferung der SMS bei DRACOON-Provider läuft über eine geschützte Verbindung; anschließend wird die Textnachricht über die übliche SS7-MAP-Verbindung zum Endgerät übertragen. Die Sicherheitsfunktionen sind somit vom genutzten Mobilfunknetz des Empfängers abhängig. Diese Funktion muss jeweils von dem Benutzer gezielt eingesetzt werden; eine automatisierte Nutzung dieses Features findet nicht statt – zumal für jeden Versand die Mobilfunknummer des Empfängers neu eingegeben werden muss.

8.8 Rechtsgrundlagen der Datenverarbeitung in DRACOON

Die für DRACOON einschlägigen Rahmenvorgaben finden sich im Landesdatenschutzgesetz und der Datenschutzverordnung Schleswig-Holstein sowie im Bundesdatenschutzgesetz (BDSG) und Telemediengesetz. Zudem sind die Rechtsprechung Europäischer Gerichtshöfe und die Auslegungshilfen der Aufsichtsbehörden zu nennen, wie z.B. Working Paper No. 196 der Artikel-29-Datenschutzgruppe („*Opinion 05/2012 on Cloud Computing*")[3] oder die „*Orientierungshilfe – Cloud Computing*" der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder[4].

Die Anwendungsbereiche von DRACOON und deren spezialgesetzliche Grundlagen können hier nicht abschließend aufgeführt werden. Um dennoch ein vergleichbares datenschutzrechtliches Schutzniveau annehmen zu können, wurde seitens der Auditoren davon ausgegangen, dass mittels DRACOON besondere personenbezogene Daten verarbeitet werden. Diese Daten unterliegen einem hohen datenschutzrechtlichen Schutz, der für die Auditierung den Prüfmaßstab bildet. Die Prüfung erfolgte am Beispiel einer Archivierung von Patientendaten, die als Gesundheitsdaten diesem besonderen Schutz unterfallen. Wesentliche Ausprägung des Patientendatenschutzes ist die ärztliche Schweigepflicht. Sie ist durch § 203 Strafgesetzbuch und § 9 der (Muster)-Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) geregelt. Damit zusammenhängend gilt ein Beschlagnahmeschutz nach § 97 der Strafprozessordnung. Soweit das Gesundheitswesen keine spezielleren Regelungen vorsieht, gilt für nicht-öffentliche Stellen ergänzend das BDSG als allgemeineres Gesetz. Für den Einsatz durch öffentliche Stellen Schleswig-Holsteins gilt das LDSG S-H. Die DSVO regelt die Dokumentation automatisierter Verfahren bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen (§ 3 Abs. 1 LDSG S-H) sowie deren Tests und die Freigabe dieser Verfahren. Für DRACOON kam es daher auf die Prüfung der Dokumentationen, Tests und Freigabeverfahren an.

---

[3] Abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/-wp196_en.pdf.
[4] Abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/orientierungshilfen-node.html .

Hervorzuheben ist, dass DRACOON im Rahmen eines Kombi-Audits gemäß DSGSVO SH und EuroPriSe geprüft wurde. Dabei wurden bereits die Anforderungen der am 27.05.2018 wirksam werdenden EU-Datenschutzgrundverordnung (DSGVO) sowie das hieraus folgende neue BDSG zugrunde gelegt und mitgeprüft. Im Ergebnis war festzustellen, dass sowohl die zum Auditzeitpunkt gültigen rechtlichen Vorgaben als auch die neuen Anforderungen bei korrekter Anwendung von DRACOON durch den Anwender eingehalten werden können.

8.9 Identifikation der Datenarten

Welche Daten an DRACOON übertragen werden, hängt vom Anwender ab; diese können personenbezogen oder -beziehbar sein, müssen es aber nicht. Aufgrund der individuellen Anwendung können die Daten nicht abschließend aufgeführt werden. Beispielhaft wurde für das Audit allerdings davon ausgegangen, dass es sich um Gesundheitsdaten handelt, so dass ein hohes Datenschutzniveau umgesetzt sein muss. Weiterhin sind Benutzerdaten als Primärdaten anzusehen, insbesondere die E-Mail-Adresse, die als Login verwendet wird sowie Anrede und Vor- und Nachname, welche im Dashboard angezeigt werden. Neben dem Audit-Log gibt es Protokolldateien, die im System von DRACOON verarbeitet werden. DRACOON schreibt jede Benutzeraktion in sein Systemlog mit, welches über das Web Frontend eingesehen werden kann. Dieses wird in der Datenbank gespeichert. Im Kontext des Syslog-Protokolls gab es ab der Version 3.3 eine weitere Neuerung, die Anwender der On-Premise-Lösung oder Anwender der Branded-Cloud--Variante (im Gegensatz zur Shared-Lösung) aktivieren können: Für diese Anwender besteht die Möglichkeit, eventuell vorhandene Syslog-Kollektoren (wie Splunk, LogRhythm, HP ArcSight) mit den Syslog-Einträgen aus DRACOON zu versorgen. In diesen Systemen ist es möglich, sich über sicherheitskritische Ereignisse in Echtzeit informieren zu lassen (z.B. fehlgeschlagene Login-Versuche). Die Funktionalität wird von der DRACOON GmbH selbst nicht angeboten, sondern lediglich die Schnittstelle hierfür. Die DRACOON GmbH bietet auch die Bereitstellung eines Syslog-Kollektors nicht als Service an; hier muss im Unternehmens-Netz und in der Verantwortung des Anwenders ein entsprechendes System vorgehalten werden. Am System selbst werden vom Webserver Logdateien angelegt. Hier werden die (auf die weniger signifikante Hälfte reduzierten) IP Adressen der Benutzer und die Zugriffszeit geloggt. Der Application Server legt die Log-Datei „catalina.out“ an. Diese enthält Informationen über den Zustand des Servers und Operationen (durch WebDAV), aber keine personenbezogenen oder personenbeziehbaren Daten. Ferner kann die Protokollierung der vollständigen IP-Adressen in der Datenbank vom Anwender aktiviert werden. Diese Einstellung ist nur in der DRACOON Branded Cloud und der DRACOON for Windows/Linux, Enterprise, OEM-Version verfügbar. Sollten IP-Adressen so gelogged werden, erkennt der Benutzer dies, indem im Dashboard von DRACOON nicht nur das Datum seines letzten Logins angezeigt wird, sondern auch die dazugehörige IP-Adresse.

8.10 Einsatzumgebung

Sofern DRACOON in einer IT-Systemlandschaft des Anwenders eingesetzt wird, hängt die Sicherheit von den Anforderungen ab, die der Anwender hier umsetzt. Hervorzuheben ist, dass der Anwender im Datenschutzmerkblatt ausreichend sensibilisiert wird, eine sichere Einsatzumgebung herzustellen. Zur Einsatzumgebung bei der DRACOON GmbH bzw. des von ihr beauftragten Rechenzentrums gehören ein Backend Server, ein Frontend Server, ein Database Server sowie ein Reverse Proxy System. Standorte, Webseiten und

öffentliche Netze der DRACOON GmbH werden regelmäßig Sicherheitsüberprüfungen bzw. externen Schwachstellenscans unterzogen. Hervorzuheben ist, dass die DRACOON GmbH im Rahmen ihres gemäß ISO/IEC 27001:2013 zertifizierten ISMS ein Risikomanagement betreibt. Ein Risikomanagementhandbuch sowie eine detaillierte Risikoanalyse wurden seitens der Auditoren eingesehen. Tests von DRACOON und seiner Komponenten werden in einem Entwicklerhandbuch beschrieben. Für Tests nutzt die DRACOON GmbH eine separate Testumgebung. Tests werden per Tool dokumentiert. DRACOON verfügt zudem über eine Knowledge-Base, die unter https://support.dracoon.com/hc/de erreichbar ist. Auf dem Portal können technische Aspekte von DRACOON als Online-Hilfe direkt aus dem Benutzerhandbuch aufgerufen werden. Zudem sind hier u.a. Benutzerhandbücher als pdf-Version zur alten und neuen Version von DRACOON abrufbar.

Die nachfolgende Abbildung illustriert Komponenten und Datenfluss:

9. Modellierung des Datenflusses

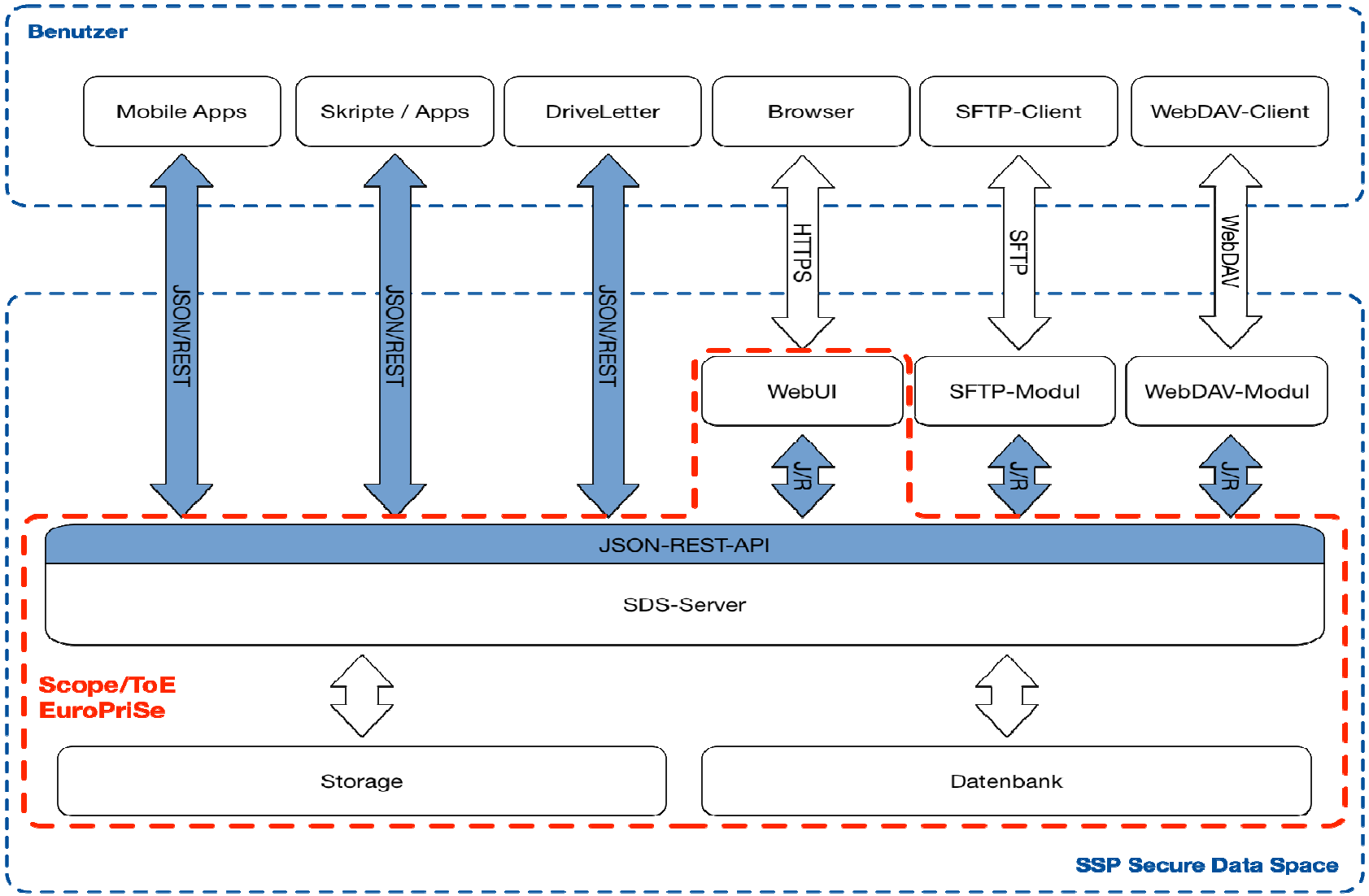


Abbildung 3: Datenfluss (SDS = DRACOON)

10. Version des Anforderungskatalogs

Version 2

11. Zusammenfassung der Prüfergebnisse

Die Prüfergebnisse im Einzelnen werden wie folgt zusammengefasst:

Anforderungsprofil für Profildaten (A)	Bewertung DSGSVO
A1 Verfügbarkeit, Integrität, Vertraulichkeit	angemessen
A2 Nicht-Verkettbarkeit	angemessen
A3 Transparenz	angemessen
A4 Intervenierbarkeit	angemessen
A5 Anpassung des IT-Produkts	angemessen
A6 Privacy by Default	angemessen
A7 Sonstige Anforderungen	nicht anwendbar
A8 Zulässigkeit der Datenverarbeitung	angemessen
A9 Einhaltung allg. Datenschutzgrundsätze	angemessen
A10 Datenverarbeitung im Auftrag	angemessen
A11 Besondere technische Verfahren	nicht anwendbar
A12 Sonstige Anforderungen	nicht anwendbar
A13 Einzelne technisch-organisatorische Maßnahmen	angemessen
A14 Allgemeine Pflichten	angemessen
A15 Spezifische Pflichten	angemessen
A16 Pflichten nach DSVO	angemessen
A17 Betrieb der Auftragsdatenverarbeitung	angemessen
A18 Sonstige Anforderungen	nicht anwendbar
A19 Aufklärung und Benachrichtigung	angemessen
A20 Benachrichtigung bei unrechtmäßiger Kenntniserlangung	angemessen
A21 Auskunft	angemessen
A22 Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung	angemessen

A23 Sonstige Anforderungen	**nicht anwendbar**
Anforderungsprofil für Profildaten (B) nach DSGSVO	**Bewertung DSGSVO**
B1 Datenvermeidung und Datensparsamkeit	**angemessen**
B2 Zweckbindung	**angemessen**
B3 Nicht-Verkettbarkeit	**angemessen**
B4 Transparenz	**vorbildlich**
B5 Rechtsgrundlagen	**angemessen**
B6 Zweckbindung	**angemessen**
B7 Aufbewahrungsfristen	**angemessen**
B8 Physikalische Sicherung	**angemessen**
B9 Zugriffsschutz	**angemessen**
B10 Ermittlung / Sichtbarkeit der Protokolldaten	**angemessen**
B11 Technische Umsetzung der Speicherfristen	**angemessen**
B12 Unzulässige Verkettung	**angemessen**
B13 Beschreibung der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit	**angemessen**
B14 Selektive Löschung von Einzeldaten, Beauskunftung, Berichtigung, Sperrung, Einwand	**angemessen**

12. Beschreibung, wie das IT-Produkt den Datenschutz fördert

DRACOON enthält folgende, den Datenschutz fördernde Funktionen:

Die Vertraulichkeit der Daten wird durch ein Berechtigungskonzept sichergestellt, das die Vergabe sehr differenzierter Zugriffsrechte ermöglicht.

DRACOON bietet dem Benutzer mit der clientseitigen Verschlüsselung die Möglichkeit, Daten absolut vertraulich per DRACOON zu speichern.

Durch Vermeidung schwacher Algorithmen bei der Verwendung von TLS für die Kommunikationsverschlüsselung wird ein hohes Maß an Vertraulichkeit erreicht.

Organisatorische und technische Maßnahmen, die der Auftragnehmer zur Datensicherheit und zum Datenschutz trifft, gehen über die gesetzlichen Anforderungen hinaus. Der

Auftragnehmer sensibilisiert den Anwender in vorbildlicher Weise auf die Einhaltung des Datenschutzes, u.a. durch ein Datenschutzmerkblatt.

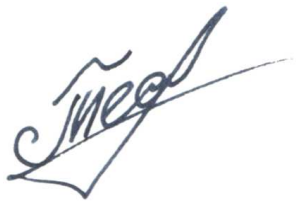
Das Rechenzentrum weist ein hohes Maß an physikalischer Sicherheit aus und ist zertifiziert.

Die seitens der DRACOON GmbH entwickelten und umgesetzten Datenschutz- und Sicherheitsmaßnahmen entsprechen vorbildlich dem Privacy-by-Design Grundsatz.

13. Votum der Auditoren

Hiermit bestätigen die Auditoren gerne, dass der DRACOON in der Version 4 (Unterversion 4.5.0) mit Funktionstand aus Januar 2018 den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Bremen, 17.01.2018



Dr. Irene Karper LL.M.Eur.
datenschutz cert GmbH

Alexey Testsov
datenschutz cert GmbH