Short Public Report

DRACOON

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

DRACOON with the following variation

- DRACOON Online
- DRACOON Branded Cloud
- DRACOON for Windows/Linux, Enterprise, OEM

Version: 4 (Subversion 4.5.0)

Functional status: 2018/01.

DRACOON is both an IT-product and an IT-based service. It was formerly known as Secure Data Space (SDS).

2. Manufacturer or vendor of the IT product / Provider of the IT-based service:

DRACOON GmbH
Galgenbergstrasse 2a
93053 Regensburg, Germany
as vendor and provider of the IT product and IT-based service.

Contact Person: Dr. Florian Scheuer, Chief Technical Officer of DRACOON GmbH.

3. Time frame of evaluation:

2017-06-06 - 2018-01-17.

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:	c/o datenschutz cert GmbH Konsul-Smidt-Str. 88a 28217 Bremen, Germany eMail: ikarper@datenschutz-cert.de
Name of the Technical Expert:	Alexey Testsov
Address of the Technical Expert:	c/o datenschutz cert GmbH Konsul-Smidt-Str. 88a 28217 Bremen, Germany eMail: atestsov@datenschutz-cert.de

5. Certification Authority:

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):

DRACOON is a web-based, virtual data room, which can be used for uploads, downloads, storage, manage and transfer of data. DRACOON is a so-called Cloud-based service.

Vendor is the DRACOON GmbH which performs development, maintenance and operation of DRACOON at the location Regensburg by order of the customer as a software as a service (SaaS) in a data center in Nuremberg, Germany.

DRACOON comes with the following variation:

- DRACOON Online
- DRACOON Branded Cloud (f.k.a. „Dedicated“)

- DRACOON for Windows/Linux, Enterprise, OEM (f.k.a. “Virtual Appliance).

DRACOON Online is the basic variation. It is offered by DRACOON GmbH as SaaS. Branded Cloud corresponds with the basic version. Additionally, it can be branded by the corporate Identity and Authentication can be realized by using the Active Directory´s. DRACOON for Windows/Linux, Enterprise, OEM is a software package. User have the choice to run DRACOON in their own IT-environment or as a SaaS by DRACOON.

DRACOON is designed for B2B. **Users** are corporations, organizations or public authorities.

Provider and vendor of DRACOON is DRACOON GmbH. The information management system of DRACOON GmbH is certified according to ISO / IEC 27001.

Subcontractor of DRACOON GmbH is ANEXIA Internetdienstleistungs GmbH, Feldkirchnerstraße 140, 9020 Klagenfurt, Austria, which is responsible for providing the VM infrastructure of the DRACOON. The work is carried out by maintenance and exchange of hardware and software in the data center in Nuremberg. ANEXIA Internetdienstdienst GmbH is certified according to ISO / IEC 27001. The data center, which is still in use at the time of the audit, will soon be replaced by Noris Network AG's data center at Thomas-Mann-Str. 16-20, 90471 Nuremberg, Germany. It is also certified according to ISO / IEC 27001.

Contracts between the DRACOON GmbH and the customer are conform to the legal aspects of data processing by an agent. Those aspects support the requirements of public data protection authorities with regard to Cloud-Computing1.

In addition, an SMS gateway and the Deutsche Telekom AG communication network are used.

---

[1] E.g. according to the „*Orientierungshilfe – Cloud Computing*“ der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder or according to Working Paper No. 196 of Article-29-Group „*Opinion 05/2012 on Cloud Computing“.*

DRACOON is accessible on the website https://dracoon.team.

Fig. 1: Login

The user defines application areas and which users get access to the DRACOON, Data Rooms and the files. For example, internal areas or individual employees but also outside the user, like other companies. The organizational structure can be represented via the data rooms (for example, special areas). DRACOON provides a detailed authorization concept for this purpose. The functions of the DRACOON are documented transparently for the user in the user's Guide.

DRACOON has the following functions:

- Expiration date for files, user accounts and download links
- Comment function for files
- Sort by user, date, type, size, name.

- Up- and downloads as zip archive
- File exchange as public download links / quick links (optionally password-protected, time-limited)
- Encrypted storage of all user data as well as all temporary passwords. for accounts or file sharing; as a result, the provider cannot access the data of the user
- Files are automatically scanned by the anti-virus scanner after upload (unless files are encrypted). If a file is infected, an attempt is made to disinfect it. If this is not successful, the file is renamed to ".virus" and the access is blocked. Automated deletion at fixed intervals removes these files permanently from the system
- Access by user accounts via e-mail address / password (default)
- Integration of the data rooms into the IT network of the user
- Easy integration as a drive (PC, MAC, LINUX)
- Configurable, temporary upload accounts for time and volume restricted access by third-party users / business partners to upload files
- All events, such as IPs, accesses, changes, uploads, etc., are optionally recorded in a revision-proof manner
- Administration and file exchange via web application (WebGUI)
- Multilingual interface: German, English, Spanish (languages are expandable)
- Backup of complete data rooms manually by Data Room Admins or DataSpace Admins or automated (via a backup agent)
- Encryption of data rooms by means of client-side encryption.

DRACOON allows the classification of confidentiality levels when uploading to

- public
- for internal use only
- confidential and
- strictly confidential.

The user can easily select the classification within his data room when processing the desired file.

In addition to the basic functionalities, **DRACOON Branded Cloud** offers the following features:

- a dedicated deployed storage environment

- a dedicated password for encrypting the storage environment,
- a branding of the environment according to the user's instructions
- login using the user's Active Directory
- DRACOON can be accessed from the Internet using any address in the context of the customer's domain. DRACOON GmbH provides a SSL certificate, if needed.

In addition to the DRACOON Online and DRACOON Branded Cloud the **DRACOON for Windows/Linux, Enterprise, OEM** provides:

- Using as an in-house solution possible
- connection to the storage provided by the user according to the DRACOON GmbH
- Use in the housing operation or in the data center of the user.

The ToE does not include:

- The use of DRACOON on Smartphones and tablets and the mobile apps,
- The operational environment
- the hardware components and in this respect the used operating system in the Datacenter
- licensing and sales processes, the company presentation https://www.dracoon.com and any further services of DRACOON GmbH.

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

Login and authentication

The user connects to the frontend via SSL and authenticates with user name and password. After the first log on to DRACOON, password must be changed. It must have at least 8 characters and consist of letters and numbers, which are automatically checked. The user is advised in a data protection data sheet to use the password protection. The leaflet is a contract component and is accessible within the account of DRACOON. However, it is possible that a different password convention is implemented at the request of the users of the DRACOON Branded Cloud and DRACOON for Windows/Linux, Enterprise, OEM. After three incorrect entries of the password at login, the user's login is blocked for three minutes. User names are stored in plain text in the database, the passwords are encrypted and stored as a Hash. DRACOON uses a well-designed authentication mechanism from the perspective of the auditors. For

standard authentication, the password is stored in the database using bcrypt / salting. The password can be resetted via e-mail, to which a link - limited to 24h validity - is sent. Here, the user can reset the password. Since version 3.3 of DRACOON, users are allowed to replace their own e-mail address used for logging and receiving messages. This does not apply if an Active Directory connection is used; in this case, the change must be made via AD. DRACOON Branded Cloud and DRACOON Windows / Linus, Experience OEM can be authenticated by connecting to one or more Active Directory at the request of the user. The user logs in with AD user name and password. The authentication process during standard installation, in which users can log on with the login data stored in the database, also remains possible. This ensures that external users who do not have an account in the AD can also use the DRACOON. Alternatively, the authentication can be performed against a radius server by token. The user logs in with user name, a PIN, and a one-time password generated by the token. The logon using the login data stored in the database is thus prevented.

Once logged in, the user accesses a dashboard as the start page

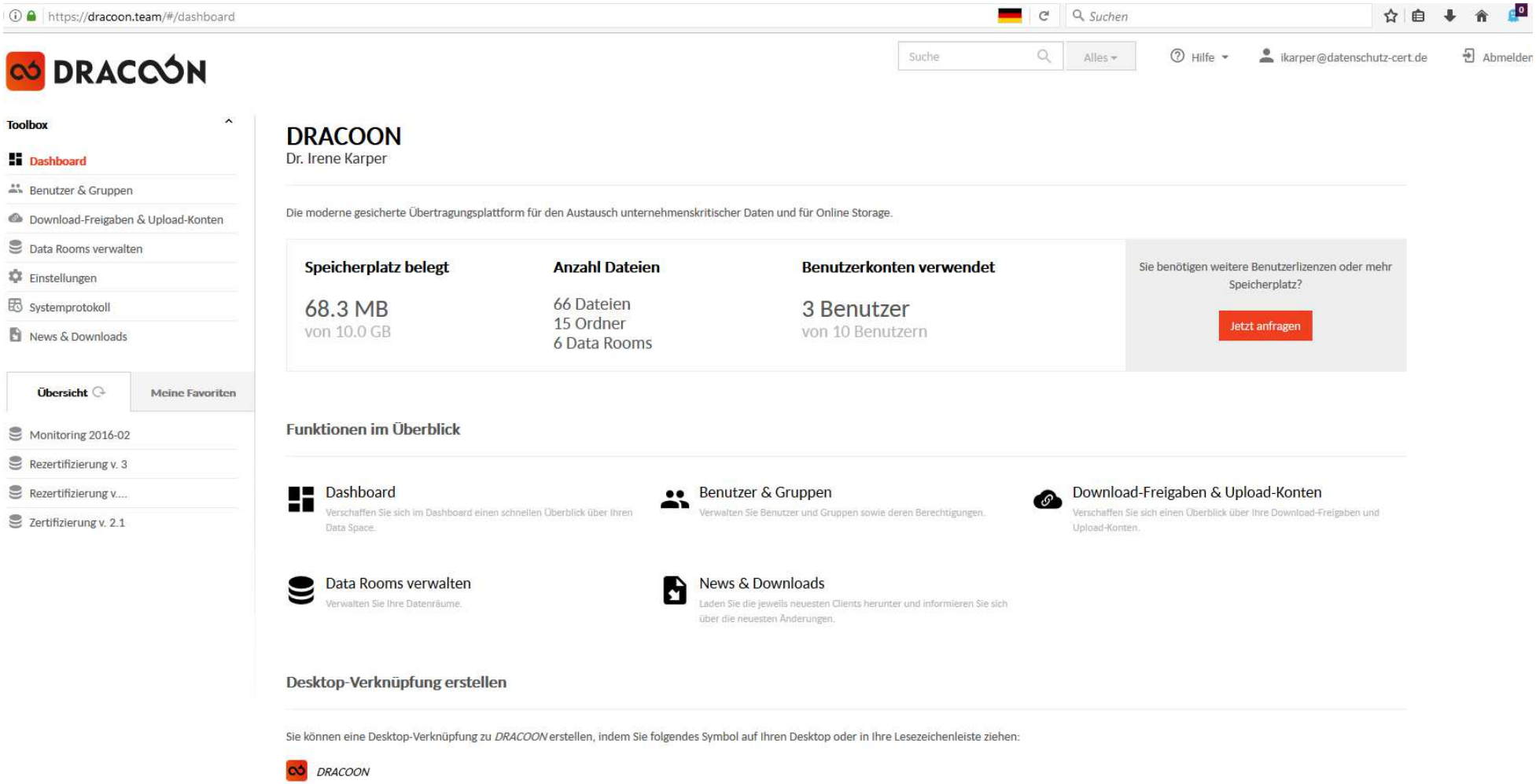


Fig. 2: Dashboard (German)

Encryption:

Data transmission between server and client is based on a SSL connection and a certificate valid at the time of the audit until October 2018. At the request of the user, DRACOON GmbH offers encryption levels of up to 256 bits, provided that web browsers and operating systems support this.

The database itself is not encrypted, but the data is stored on LUKS encrypted disks within the secured data center. Optionally, data can be encrypted on the client side prior to transmission to the data room. In this case the encryption is always for the entire data room and has to be performed when the data room is empty. When using an encrypted data space for the first time, every user has to choose an encryption password from which a key pair (RSA-2048) is generated. This key pair is used in all encrypted data rooms of this data space. A random symmetric key (AES256) is generated by using Galois Counter Mode (GCM) for any document that is filed here to encrypt the document. This symmetric key is then encrypted with the public key of all users being eligible for the data room and placed along with the encrypted data in the database. Thus, all users who have a data room read permission can read all data in the data room, even if they are encrypted. If only one user shall have a read permission, it is possible to create an individual sub rooms. To read an encrypted file, the user is prompted to enter his encryption password with which the private key is released to decrypt and use the symmetric key. The encryption and decryption operation is performed via JAVA script and Java applet in the browser of the DRACOON user on the client. The keys are requested from the database of the DRACOON and held in the memory of the client. Using this client-side-encryption there is no file unencrypted on the DRACOON back-end systems available and thus no administrator of DRACOON GmbH can read the data not even in transit.

With version 3.9 of DRACOON the encryption possibilities were extended. With upload accounts, the external user is supplied with the public key of the creator. Thus, encryption of the file is easy for external users. It does not reveal which and how many other users have permissions on the data space. The public key provided does not carry any identity information from the owner, so it is not a certificate in particular. For download links, a separate key pair is created, for which a copy of the file key is provided in the usual way. The release password of this link protects the newly generated private key on cryptographic basis and thus creates an analogue to the encrypted password of the registered user. The external user has to enter this password when using the release link connection, the web interface decrypts the private key with the already used internal functions

and then the file (using the individually encrypted file key ("FileKey"). Without knowing the password, the platform operator cannot see the encrypted data files shared via release link.

DRACOON offers the possibility to establish rescue keys for the case of emergency. If triple-crypt is enabled, the data space admin has the ability to set up a rescue key. When a new data room is created, the admin has the ability to decide whether rescue keys are used for this data room of the data space or not. The rescue keys are key pairs for asymmetric encryption and do not differ from the user key pairs. The private key is protected by a long and complex password, which is protected by the appropriate role (data space admin or data room admin) using suitable organizational measures. When a rescue-key is used, all symmetric file-keys of data rooms are encrypted with the entire legitimate user and the appropriate rescue public keys, and stored in the database. Using a data space rescue key, it is ensured by the authorization concept that a data space Admin can only access data, which have been released by the respective data room admin for him - even with knowledge of the data space rescue key. The rescue keys serve as safety anchor, for the case that all users of a data room have forgotten their encryption passwords. With the help of the rescue keys, the data is then still decodable. If no rescue key is used, the data can no longer be decrypted.

Deletion of data, data minimization, portability

Deletions are contractually regulated between the DRACOON GmbH and the user. Primary data can be deleted by the user himself manually or by setting a deletion date (expiration date) when uploading. In the latter case, the selected files are deleted completely after the deletion deadline via cronjob. Associated secondary data, such as change logs remain up to termination of the contract between DRACOON and the user. Log data, which serve as an attack detection, are deleted after 7 days, unless otherwise instructed. At the user’s request log data can be deployed longer. Therefore, a separate contract is required. The normal retention period is then usually three months. With version 3.2, a new paper basket function was introduced, in which the Data Room Admin can define a period of time in which files are automatically removed. Version 3.8 allows Data Space Admin to define the data volume ("quota") to be stored there when creating a data room. If the volume is exceeded, no upload is possible until space has been released. Upon termination, the user is given the option of exporting all data via zip archive.

Activity Log

With version 3.9 of DRACOON, an activity log is provided for each data space to allow authorized users an aggregated view of the modifications of files (e.g. new, modified or deleted files). Only file operations are logged, which a user could view anyway by means of the meta information of the objects. The Activity Log is therefore only a more comfortable form of processing. It is also possible to disable the Activity Log globally.

Audit Log

Data Space Administrators can look for, view and understand transactions carried out by users in his data space with the help of the audit log. The audit log cannot be changed and can only be deleted by deletion of the client.

Components and interfaces:

DRACOON has the following components:

- WebUI
- JSON-REST-API-Schnittstelle
- DRACOON-Server
- Management Database.

It can be accessed via standard Web browsers. DRACOON can also be accessed through mobile devices (smartphones, tablets**). Apps and mobile devices are not part of the ToE.**

In addition, DRACOON can be integrated as a drive via the WebDAV interface, but then without the client-side encryption. There is a leaflet with privacy instructions (privacy leaflet) in which the user is made aware, only to use trustworthy clients. In particular, it undeceives the user about a possible criminal liability for unlawful disclosure with respect to professional secrecy.

With the versions 3.4 and 3.5 of the DRACOON, the configuration of the API interface for improved integration of the AD was re-established. The DRACOON server has a JSON-REST-API that builds functionality of software. Functionality and logic of data proceeding has changed from clients to server side. This API is now the only gateway to applications, implemented in the DRACOON. Therefore, all clients have the same security and data protection measures. Clients have only

logical functions which are necessary for picturing information on screens, integration of DRACOON in systems and workflows and for encryption. Standard client is a WebUI. This client gives the full functional standard and is hosted in the data center of DRACOON Ltd. This WebUI has no server-side logic (as known by classic web applications PHP or JSP) but it runs the surface by JavaScript within the web browser of the client. To get this information, the client communicates directly with the API. All further gateways, that are not part of the target of evaluation and certification, were also operated by the JSON_REST_API. For WebDAV and SFTP gateway a proxy was implemented to map communication of clients and API, using the provided protocol.

DRACOON has the following interfaces:

- https-access over WebIU
- internal MySQL data base gateway
- Java/IO function for local mount and data-storage
- smtp for eMailing (mailing link for download function)
- API gateway
    - sftp gateway via API
    - WebDav gateway (for implementation of hardware) via API
    - Gateway for mobile devices and Drive Letter

Permissions and roles

Permissions can be assigned gradually according to the roles and functions:

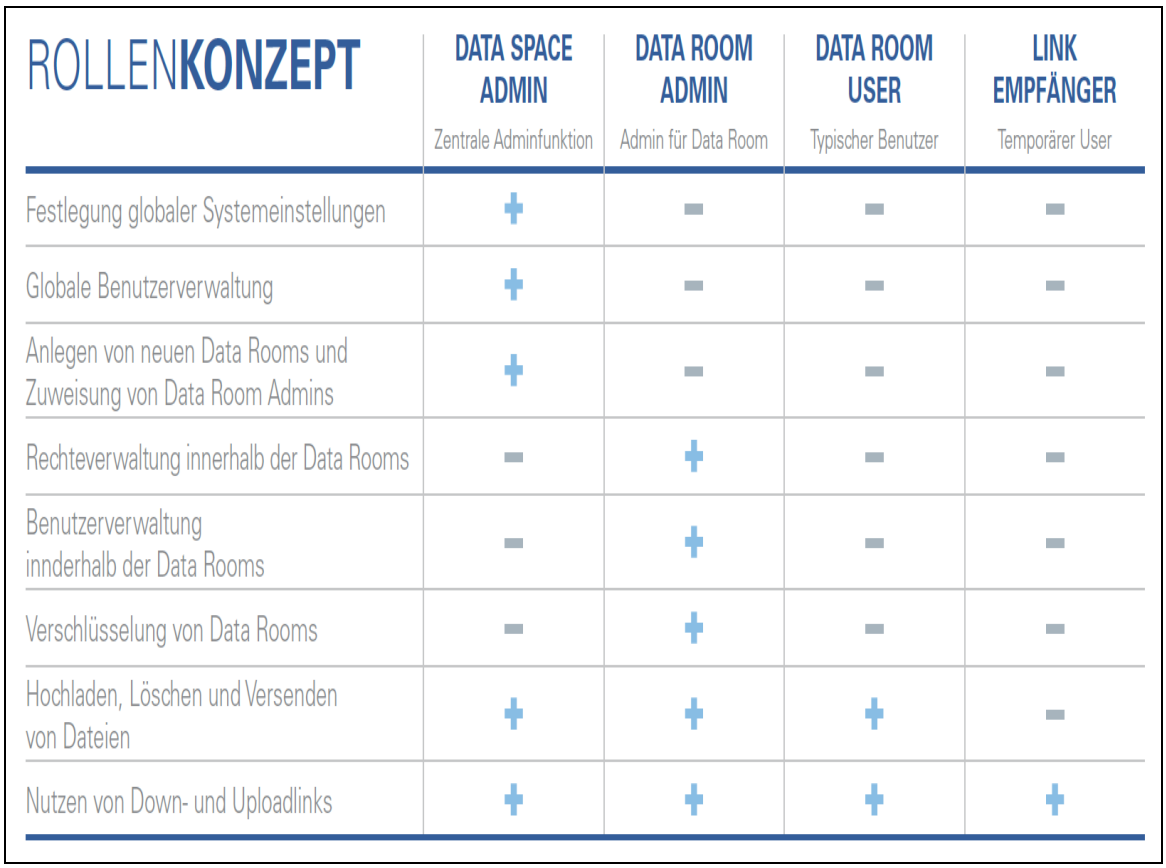


Fig. 3: Authorization concept (German)

Data Space Admin

The DataSpace Admin has the central administration function of the user account with an overview as well as all rights to the Data Space Rooms and subrooms as well as the user / rights management. With version 4.0 of DRACOON, a division was made in five roles: Config Manager, Room Manager, User Manager, Group Manager and Log Auditor, each of which can be assigned separately to users and user groups.

Data Room Admin

The Data Room Admin is the administrator of the respective data rooms. He has an overview of the user, the user rights (upload, delete, data room admin), he can create subrooms and can edit assignments of unassigned users to his data rooms (add, remove added users). He can be data room admin and data room user at the same time in different data rooms / subrooms. Version 3.0 of DRACOON now gives the data room admin the possibility to activate client-side encryption easily by one click. Since version 3.9, the Data Room Admin can individually define an

initial data space for each user, which is displayed to the user directly after the login instead of the dashboard.

Data Room User

The data room user can upload, delete, and sent download links in his account, mark as a favorite, search (depending on the rights granted) and - depending on the user's requirements – have the role of a Data Room Admin. It is also possible to inherit rights to data spaces at lower hierarchical levels. This is necessary for a Data space structure, which can now extend over many levels, since the respective individual configuration of all authorizations of all users at each level can represent a tremendous source of error. With version 4.0 of DRACOON, the previous restriction was lifted that data spaces can only be created on the two top layers. As a result, all the structures of a company can be mapped via data spaces. A drag-and-drop function for files has also been introduced. By selecting files, a new "Notify" button can be used to easily create an e-mail containing references to the selected files. This allows the user to conveniently send notices to other users.

Link recipient and upload account

Users of the download links or the users of the upload account do not need an own account with the DRACOON. The links consist of a random character combination, so that no conclusions can be made with the numbering or similar. The release link receives 32 digits (A-Z, a-z, 0-9). There are 6232 (order of magnitude: 1057) different links, which in addition (as usual) with a password can be protected. It is easy to create different release links (with different passwords and expiration dates) for the same file. Thus, different users get different links and do not need to know or reuse the same password. The maximum number of downloads of a release link can be determined, e.g. to the maximum number of 1. This makes the data inaccessible after the first use. If the download is no longer usable, it can be seen that the information has been downloaded without authorization and has to be considered as betrayed.

Optional: Enable the password via SMS

If a release link is password-protected, then the user has been given the option to have the selected password sent via SMS as of version 4.1 of the DRACOON. The mobile phone number of the receiver must be provided for this purpose. The user

must first activate this function in the system settings. This feature has been supplemented so that the secret is shared: On the one hand the link is still sent in the e-mail, otherwise the password is transmitted via a second channel as SMS. This function is only possible with unencrypted files; because when the encrypted files are released, the server is not allowed to gain any knowledge of the password as otherwise the end-to-end principle would be violated. If this function is used, the server generates a short message which, in addition to a simple note, contains the password and sends it to the mobile phone number entered by the user. The only information provided is a MSISDN as well as the chosen password - in this case, however, with no associated random link. That the download of the file is also not possible due to the knowledge of the short message; one is dependent on the random link (about 192 bits of entropy) transmitted via another channel (in the form of an e-mail). A gateway from Deutsche Telekom AG is used for the SMS dispatch. The transmission of the SMS with DRACOON provider runs over a protected connection; then the text message is transmitted to the terminal via the usual SS7-MAP connection. The security functions are thus dependent on the used mobile radio network of the receiver. This function must be used by the user; an automated use of this feature does not take place - especially since the mobile phone number of the recipient has to be re-entered for each shipment.

Legal basis of data processing in DRACOON

The framework conditions applicable to the DRACOON can be found in the Data Protection Act of Schleswig-Holstein (LDSG S-H), the Data Protection Ordinance Schleswig-Holstein (DSVO) as well as in the Federal Data Protection Act (BDSG) and Telemedia Act (TMG). It should be emphasized that the DRACOON has been checked as part of a combi-audit in accordance with Privacy Seal Regulation S-H and EuroPriSe. The requirements of the EU Data Protection Regulation (DSGVO), which will be applicable as of 25.05.2018, as well as the following new Federal Data Protection Act (BDSG were already taken into account and tested. In addition, the jurisprudence of the European Court of Justice and the interpreting aids of the supervisory authorities, Working Paper no. ("Opinion 05/2012 on Cloud Computing"), or the "Cloud Computing" orientation work of the Technology and Media Working Group of the Data Conference Protection Commissioners of the Confederation and the States of Germany.

The fields of application of the DRACOON and its special legal bases cannot be listed here. In order to nevertheless be able to accept a comparable level of data

protection, the auditors have assumed that personal data are processed using the DRACOON. These data are subject to a high level of data protection, which forms the test bench for auditing purposes. The examination was carried out in the form of an archiving of patient data which, as health data, is subject to this particular protection. The essential characteristic of patient data protection is medical confidentiality. It is governed by § 203 of the Criminal Code and § 9 of the (template) – professional code for the German physicians (MBO-Ä). Accordingly, a seizure protection according to § 97 of the Criminal Procedure Code applies. Provided that there is no specific regulation, the BDSG as a more general law applies to non-public bodies. The LDSG S-H is valid for use by public authorities in Schleswig-Holstein. The DSVO regulates the documentation of automated procedures for the processing of personal data by public authorities (§ 3 Abs. 1 LDSG S-H) as well as their tests and the approval of these procedures. For the DRACOON, therefore, the examination of the documentation, tests and release procedures was considered.

As a result, it was noted that the correct user of the DRACOON can be compliant with both, the legal requirements applicable at the time of the audit and the new requirements.

Identification of data

The data that is transferred into the DRACOON, depends on the user; this can of course be personal or person-related data. Due to the individual usage, the data can be not finally listed. It was assumed for the evaluation that it could be health data, so that a high level of data protection had to be implemented. User data is identified as primary data - in particular the e-mail address that will be used as login, title and first and last name, which appear in the dashboard.

In addition to the audit log, there are log files that are processed in the DRACOON system. The DRACOON writes each user action into its system log, which can be viewed via the Web front end. This is stored in the DRACOON database. In the context of the syslog protocol, there was another innovation from the version 3.3 of the DRACOON that users of the on-premise solution or users of the branded-¬Cloud variant (in contrast to the shared solution) can activate: For these users it is possible to supply any syslog collectors (such as Splunk, LogRhythm, HP ArcSight) with the syslog entries from the DRACOON. In these systems, it is possible to obtain information about security-critical events in real-time (e.g., failed

login attempts). The functionality is not offered by DRACOON GmbH itself, but only the interface for this. DRACOON GmbH does not offer the provision of a syslog collector as a service; an appropriate system must be maintained in the company network and the responsibility of the user. The web server creates log files for the system itself. Here the IP addresses of the users (reduced to the less significant half) and the access time are logged. The application server creates the log file "catalina.out". This contains information about the state of the server and operations (through WebDAV), but no personal or person-related data. Furthermore, the logging of the complete IP addresses in the database can be activated by the user. This setting is only available in the DRACOON Dedicated or DRACOON Virtual Appliance versions. If IP addresses are logged, the user recognizes this by not only displaying the date of his last login in the DRACOON dashboard but also the associated IP address.

Operating environment

If the DRACOON Virtual Appliance is used in an IT system landscape, the security depends on the requirements that the user implements. It should be emphasized that the user is sufficiently sensitized in the data protection note to produce a safe environment. A backend server, a front-end server, a database server as well as a reverse proxy system are part of the deployment environment at DRACOON GmbH and / or the data center commissioned by it. Sites, websites and public networks of DRACOON GmbH are regularly subjected to security checks or ex - ample weaknesses. It should be emphasized that DRACOON GmbH operates a risk management system within the scope of its ISMS certified according to ISO / IEC 27001: 2013. A risk management manual as well as a detailed risk analysis were included on the part of the auditors. Tests of the DRACOON and its components are described in a developer manual. For tests, DRACOON GmbH uses a separate test environment. Tests are documented by a tool. The DRACOON also has a knowledge base, which can be reached at https://support.dracoon.com/hc/de. On the portal, technical aspects of the DRACOON can be called up as online help directly from the user manual. In addition, User manuals as a pdf version of old and new versions of DRACOON.

8. Transnational issues:

Since DRACOON is a web-based application it can be used worldwide. Organisations deploy DRACOON at their branches within the EU, the EEA or worldwide. System and servers of DRACOON are located within the Federal

Republic of Germany and are managed by DRACOON GmbH on behalf of the user. All components of DRACOON as well as the associated maintenance services are carried out within the Federal Republic of Germany.

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

None.

10. Edition of EuroPriSe Criteria used for the evaluation:

Version January 2017.

11. Modifications / Amendments of the IT product or IT-based service since the last (re)certification

New functionalities since the last certification:

Directories can now be shared.

Introduction of a recycle bin where old versions of files can be kept.

The syslog entries can now optionally be sent to an audit system (e.g., Splunk).

E-mail addresses can be changed by the users.

Customers' Accounts can be locked.

Favorites: Files and folders can be tagged as favorites by users for quick access

Upload accounts can be password protected.

Upload accounts and download links (with password protection) in encrypted rooms were enabled.

The Activity Log has been introduced, allowing authorized users to see, etc. which new files have been added in their rooms.

Granular rights concept and new roles.

Sending release passwords via SMS.

Drag and drop upload via the web interface.

Sending note e-mails via the web interface.

Publicly uploaded files can now be hidden.

12. Changes in the legal and/or technical situation

None.

13. Evaluation results:

DRACOON is – in the opinion of the EuroPriSe expert´s –a save data room which fulfills the requirements of data protection and IT-security. Information on DRACOON is easily accessible, significant and gives further hints to usage and configuration of the DRACOON in an optimal and privacy-friendly way.

The user of the DRACOON is responsible to observe the data protection requirements and to put to use when uploading, storing, or forwarding of data by means of the DRACOON. The data protection requirements may vary depending on the user and the task environment. The DRACOON supports him in compliance by hints and recommendations. In accordance with these hints, there is no concern that the DRACOON can be used meeting the requirements of data protection.

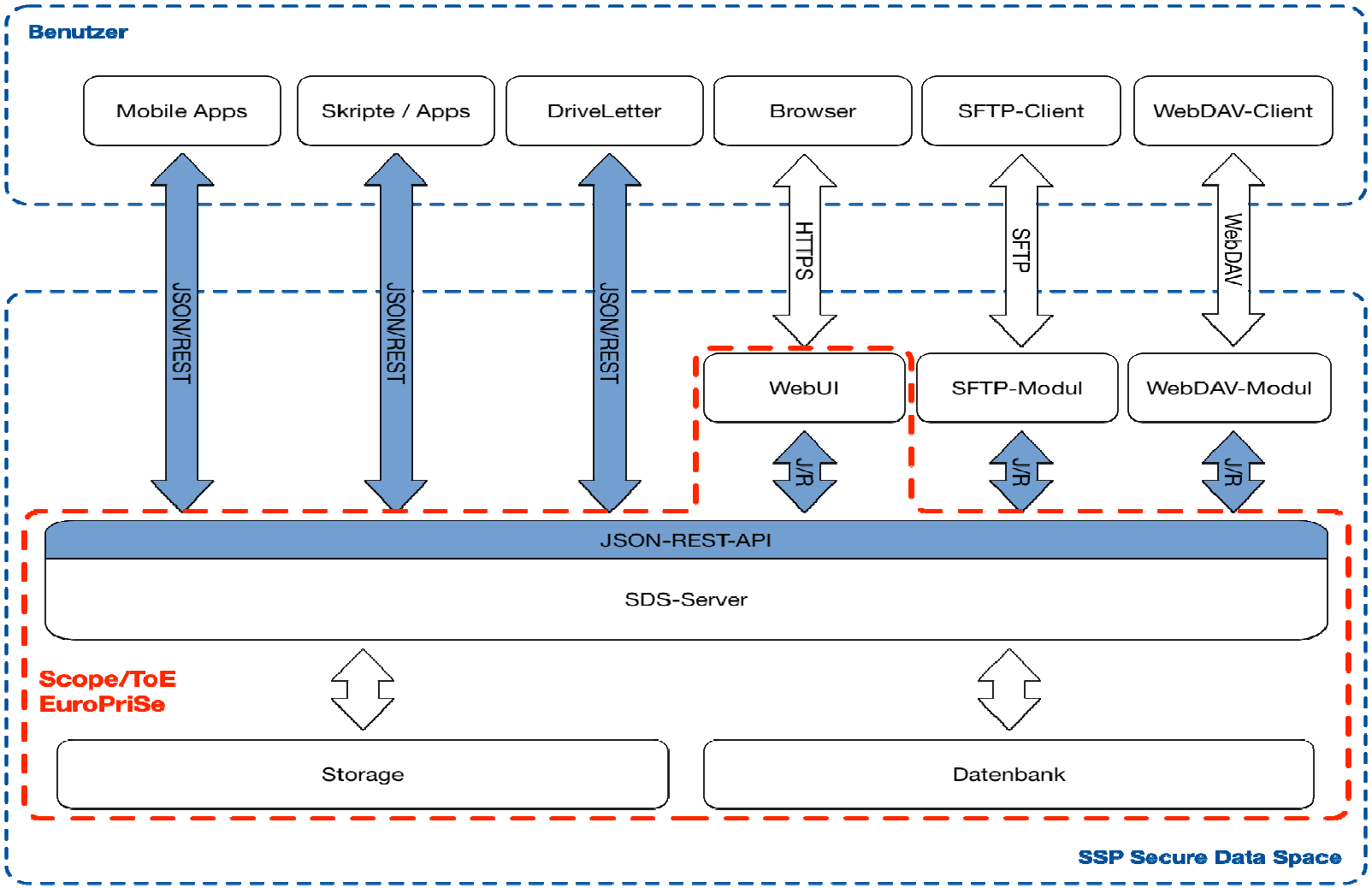
Technical and organizational security measures at the DRACOON GmbH and their service providers are carefully and appropriately implemented and regularly checked. They are verified by the valid certifications of the relevant systems and processes by an independent third body. Operational guidelines govern the application of security measures and the handling of possible deviations. Strong encryption mechanisms are used to ensure the confidentiality of the data in the DRACOON. In particular, the possibility of the client-side encryption offers the user the possibility to exclude the reading of data by unauthorized persons. The DRACOON GmbH nor its service providers can read data that is kept encrypted by the user in its DRACOON. This meets the strict requirements concerning the protection of patient data or other specific personal information. The algorithms used correspond to the current state of the art. The confidentiality and purpose of data is also ensured by the authorization concept, which allows setting differentiated access rights.

Log data and system protocols are used data-minimizing but also effectively to protect the relevant systems. The user is sensitized to privacy measures by using optional add-ons, in particular by the data protection information sheet (privacy

leaflet). Comprehensive monitoring, SPAM filter and recovery measures assure the availability of data within the DRACOON. Websites are encrypted by https. The transport of data while using web-forms is protected. The visitor of the website is informed about the use of cookies (session-cookies are used) in the privacy statement. The IP-address is anonymized.

It is to stress out that the rights of data subjects must be claimed against the customer which processes data on his own liability. The customer has been sensitized by documents and further information about data protection, available at the customers DRACOON account. DRACOON GmbH has a privacy protection officer who is to be contacted for privacy aspects. He supports both, customers and data subjects regarding their data protection rights.

14. Data flow:


Benutzer
Mobile Apps
Skripte / Apps
DriveLetter
Browser
SFTP-Client
WebDAV-Client
JSON/REST
JSON/REST
JSON/REST
HTTPS
SFTP
WebDAV
WebUI
SFTP-Modul
WebDAV-Modul
J/R
J/R
J/R
JSON-REST-API
SDS-Server
Scope/ToE
EuroPriSe
Storage
Datenbank
SSP Secure Data Space

15. Privacy-enhancing functionalities:

DRACOON has the following privacy enhancing functionalities:

An authorization concept, which allows the use of differentiated access rights, ensures the confidentiality of the data.

DRACOON provides the user with the ability to save data absolutely confidentially by DRACOON by using client-side encryption.

Avoiding weak algorithms with the use of TLS for encrypted communication, achieves a high degree of confidentiality.

Organizational and technical measures affecting data security and privacy go beyond the legal requirements: DRACOON GmbH sensitizes the user in an exemplary way on compliance with data protection, including through a data protection leaflet.

The data center, in which the components of DRACOON are located, shows a high degree of physical security and is certified.

The data protection and security measures developed and implemented by DRACOON GmbH are exemplary in accordance with the privacy-by-design principle.

16. Issues demanding special user attention:

The evaluation did not rate any of the issues as “additional safeguards needed”. Nevertheless, the privacy compliant use of DRACOON lies within the responsibility of the user. He must adopt the given information by the developer (e.g. data protection fact sheet).

17. Compensation of weaknesses:

Since DRACOON does not pass any requirement with the grade “barely passing”, there is no need to compensate a shortcoming.

18. Decision table on relevant requirements:

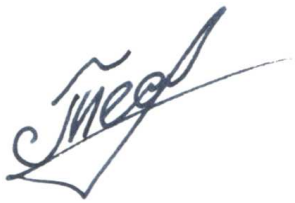
EuroPriSe *Requirement*	*Decision*	*Remarks*
Data Avoidance and Minimization	*adequate*	The user of the DRACOON controls the data storage itself. He is adequately sensitized on the adherence to the principles of data minimization and prevention.
Transparency	*excellent*	Product documentation, privacy statement and the data protection instructions are informative, up-to-date and transparent and provide good guidance in the implementation of the DRACOON.
Technical-Organisational Measures	*adequate*	Technical and organizational security measures at the DRACOON GmbH and their service providers are carefully and appropriately implemented and checked regularly. They are verified by the valid certifications of the relevant systems and processes by an independent third body. Operational guidelines govern the application of security measures and the handling of possible deviations.
Data Subjects' Rights	*adequate*	The user is appropriately sensitized on the compliance with the rights of the person concerned including the information that is available to him within his account. The DRACOON GmbH has appointed also a corporate privacy officer, who acts as contact person in privacy matters and inquiries about privacy concerning DRACOON.

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, 2018-01-17 Dr. Irene Karper LLM.Eur.

Place, date	Name of Legal Expert	Signature of Legal Expert



Bremen, 2018-01-17 Alexey Testsov

Place, date	Name of Technical Expert	Signature of Technical Expert

Certification Result

The above-named IT product / IT-based service passed the EuroPriSe evaluation.

It is certified that the above-named IT product / IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

Place, Date	Name of Certification Authority	Signature