

Allgemeine Geschäftsbedingungen, Datensicherheits- und Datenschutzbestimmungen und Sicherheits- und Nutzungshinweise **dDataBox**



Allgemeine Geschäftsbedingungen

Es gelten die allgemeinen Geschäftsbedingungen von Dataport in der bei Vertragsschluss jeweils geltenden Fassung. Unsere Allgemeinen Geschäftsbedingungen sind im Internet unter www.dataport.de veröffentlicht.

Besondere Nutzungs-, Datensicherheits- und Datenschutzbestimmungen

Der Auftraggeber ist bei der Nutzung für die Einhaltung der für ihn bzw. für die von ihm verarbeiteten Daten geltenden Gesetze und Regelungen verantwortlich, insbesondere für die gesetzlichen Anforderungen an die Verarbeitung personenbezogener Daten und für Anforderungen an Vertraulichkeit bzw. Geheimschutz. Der Auftraggeber ist für die Ermittlung des Schutzbedarfes und für die Prüfung, ob die **dDataBox** geeignet ist, diese Anforderungen zu erfüllen.

Der Auftraggeber ist dafür verantwortlich, dass die **dDataBox** in einer Weise genutzt wird, die mit den rechtlichen Verpflichtungen des Kunden im Einklang steht.

Der Auftraggeber ist für die Einhaltung von Immaterialgüterrechten verantwortlich, d. h. dass Inhalte nur hochgeladen, heruntergeladen oder freigegeben werden, wenn die erforderlichen Nutzungsrechte vorliegen.

Die Nutzung von der **dDataBox** für folgende Zwecke bzw. Inhalte ist untersagt:

- Unaufgefordertes Versenden von Mitteilungen, Reklame oder Werbung,
- Veröffentlichung oder Freigabe von rechtswidrig pornographischen oder unsittlichen Inhalten oder von Inhalten, die Gewalttaten oder terroristische Aktivitäten, einschließlich Terrorpropaganda, enthalten,
- Befürworten von Hass oder Diskriminierung von Personen oder Personengruppen aufgrund ihrer Religion, ethnischen Herkunft, ihres Geschlechts, ihrer Geschlechtsidentität, sexuellen Orientierung, Behinderung oder Beeinträchtigung
- Jegliche Gesetzesverstöße, einschließlich Speicherung, Veröffentlichung oder Freigabe von Inhalten, die betrügerisch, diffamierend oder irreführend sind oder die Privatsphäre oder Rechte anderer verletzen.

Sofern die Triple-Crypt Verschlüsselung aktiviert ist, entspricht die Lösung den IT-Sicherheitsanforderungen des BSI IT-Grundschutz hoch, mit Einschränkung der Verfügbarkeit, die normal ist.

Bei der Verarbeitung personenbezogener Daten hat die Aktivierung der Triple-Crypt-Verschlüsselung zu erfolgen. Die Verantwortung zur Prüfung und Beurteilung, welche Daten verarbeitet werden können, liegt beim Auftraggeber.

Die Verantwortung des Auftraggebers zur Einhaltung der Bestimmungen umfasst alle angelegten Benutzer.

Das der **dDataBox** zugrunde liegende Software-Produkt trägt den Namen DRACoon.

Sicherheits- / Nutzungshinweise

Endgeräte (Clients)

Hinweis auf mögliche Endgeräte: Mobile Devices, Notebook, Smartphone, Desktop

Unsere Empfehlung:

Es sollten (insbesondere bei Smartphones) gemanagte Geräte mit Virenschutz verwendet werden. Idealerweise unterliegen die Geräte noch weiteren Sicherheitsrichtlinien.

Protokollierung

In der **dDataBox** werden durch die Nutzung auf den verschiedenen Ebenen Protokolle (z.B. An- und Abmeldung bei der **dDataBox**, Datei Up- und Downloads, Logins und Login-Versuche, Benutzerberechtigungen) erstellt. Die Protokolle enthalten zum Teil personenbezogene Daten. Diese Log-Dateien sind gemäß den gültigen Vorschriften datenschutzrechtlich zu behandeln. Einen Zugriff auf die Log-Dateien haben lediglich die jeweiligen **dDataBox**-User mit der Rolle und „Auditor“.

Verschlüsselung

In der **dDataBox** werden verschiedene Verschlüsselungstechnologien eingesetzt, deren Kombination als *Triple-Crypt® Technology* bezeichnet wird.

- auf dem Transportweg mittels SSL/TLS (Channel Encryption)
- zusätzlich bei der Speicherung in verschlüsselten Dateisystemen (Server Side Encryption)
- sowie optional clientseitig, um eine echte Ende-zu-Ende-Verschlüsselung zu realisieren (Local Encryption)

Für eine clientseitige Verschlüsselung der einzelnen Datenräume muss der **dDataBox**-Administrator einmalig die Verschlüsselung für die **dDataBox** aktivieren, damit die Datenraum-Administratoren einzelne Datenräume optional verschlüsseln können.

Einschränkung für verschlüsselte Datenräume

Wurde die *Triple-Crypt® Technology* für einen Datenraum aktiviert, so sind die folgenden Funktionen für den jeweiligen Datenraum nicht mehr verfügbar:

- Das Kopieren und Verschieben von Dateien in unverschlüsselte Datenräume (für die die *Triple-Crypt® Technology* noch nicht aktiviert wurde).
- Das Freigeben des ganzen Datenraums oder eines Ordners zum Download (einzelne Dateien können jedoch zum Download freigegeben werden).


















Das Herunterladen mehrerer Dateien, Ordner oder des ganzen Datenraums als gebündeltes Zip-Archiv.

Allgemeine Geschäftsbedingungen, Datensicherheits- und Datenschutzbestimmungen und Sicherheits- und Nutzungshinweise dDataBox



Rechte und Rollen

In der dDataBox findet ein umfangreiches Rechte und Rollenmanagement Anwendung.

				
	Link Empfänger	Datenraum Benutzer	Datenraum Administrator	dDataBox Administrator
Rollenkonzept	temporärer Benutzer	typischer Benutzer	Administrator für Datenräume	zentrale Administrator-Funktionen
Nutzen von Down- und Uploadlinks				
Hochladen, Löschen und Versenden von Dateien				
Secure-Private-Room-Funktion (kein Zugriff auf die Inhalte innerhalb des Datenraums durch den dDataBox Administrator)				
Benutzer- und Gruppenweisungen innerhalb von Datenräumen				
Anlegen von neuen Datenräumen und Zuweisung von Datenraum-Administratoren				
Globale Benutzerverwaltung				
Aktivierung der TripleCrypt-Verschlüsselung				
Teilaufgabendelegation in Form der Manager-Rollen				

- **dDataBox-Administrator:** Der dDataBox-Administrator verfügt zusätzlich über alle fünf Management-Rollen. Der dDataBox-Administrator kann nicht auf einen Datenraum zugreifen, sofern er hierzu nicht berechtigt wird. Er selbst kann nur bei der Erstanlage eines Datenraums eingetragen werden. Später kann er nur durch einen Datenraum-Administrator hinzugefügt werden.
- **Konfigurationsmanager:** Festlegung der Systemeinstellungen (allgemeine Aktivierung der Triple-Crypt® Technology)
- **Benutzermanager:** Kann Benutzer anlegen, bearbeiten und löschen
- **Gruppenmanager:** Kann Benutzergruppen anlegen, bearbeiten und löschen. Er kann außerdem Benutzer an Gruppen zuweisen
- **Raummanager:** Kann Datenräume (erster Ebene) anlegen, umbenennen und löschen; Der Raummanager kann Speicherplatzbeschränkungen der Datenräume festlegen (Quotas).
- **Auditor:** Kann Einsicht in das Systemprotokoll nehmen
- **Benutzer:** Kann die Funktionalitäten in den Datenräumen anwenden
- **Link Empfänger:** Kann mittels Download- oder Uploadlinks Dateien transferieren. Benutzer können auf bestimmte Managementaufgaben ermächtigt werden.