drkserver

Deutsches Rotes Kreuz

# Datenschutz im drkserver – eine Einführung

2018
29. Mai

Der Datenschutz im drk**server** ist von hoher Bedeutung. Weil zum Teil sensible Personendaten erfasst, verarbeitet und genutzt werden, müssen im Umgang mit dem drk**server** größte Sorgfalt und ein rechtlich einwandfreies Vertragsverhältnis angewandt werden.

In aller Ausführlichkeit können Sie die Informationen zum Datenschutz im passwortgeschützten Handbuch nachlesen. Mit diesem Tipp erhalten Sie eine kompakte Übersicht mit Verweisen auf das Handbuch, auf Hilfetexte im drk**server** sowie Beispiele aus dem DRK-Alltag.

Diese aktualisierte Version des Tipps berücksichtigt die Anpassungen im Rahmen der Einführung der EU-Datenschutzgrundverordnung (EU-DSGVO).

## 1 Ihre Daten im drkserver

### 1.1 Zentrale Datenverarbeitung: Warum drkserver?

Eine wichtige Aufgabe des DRK ist die Hilfeleistung in Notfällen und Katastrophen. Dies erfordert – ganz im Sinne des Komplexen Hilfeleistungssystems des DRK – eine zentrale Datenverarbeitung, um in Krisen- und Notfallsituationen schnell und angemessen reagieren zu können.

- Mehr zur zentralen Datenverarbeitung:
  https://www.drkserver.org/3585/datenschutz > Informationen zur Datenverarbeitung
- Mehr zum Komplexen Hilfeleistungssystem:
  Handbuch > Einleitung > Komplexes Hilfeleistungssystem

### 1.2 Gespeicherte Daten: Was weiß der drkserver über mich?

Die Daten, die Sie angegeben haben, als Sie die Mitgliedschaft im DRK erworben haben, sollten im drk**server** erfasst sein. Wenn Sie während Ihrer Mitgliedschaft weitere Daten erwerben – zum Beispiel über Lehrgänge, Fortbildungen und Einsätze –, sollten ganz im Sinne des Komplexen Hilfeleistungssystems auch diese Informationen erfasst werden.

- Mehr zu den Daten, die über Sie gespeichert werden:
  https://www.drkserver.org/3585/datenschutz > Informationen zur Datenverarbeitung, Kapitel 1

### 1.3 Gespeicherte Daten: Wer hat Zugriff?

Die einzelnen DRK-Verbände/-Einrichtungen haben in dem Umfang Zugriff auf diese zentral gespeicherten Daten, wie dies für die Aufgabenerfüllung der jeweiligen Stelle erforderlich ist. Auch weitere DRK-Verbände/-Einrichtungen dürfen diese Daten verwenden, sofern es für deren konkrete Aufgabenerfüllung nötig ist. Dies wird über ein ausführliches Rollen-/Rechte-Konzept gesteuert und über ein Zugriffsberechtigungs-konzept festgelegt.
Wer was wann an Ihren Daten geändert hat, sehen Sie in Ihrer Akte im Bearbeitungsprotokoll (oben rechts:  )

- Mehr zur Zugriffsberechtigung:
  https://www.drkserver.org/3585/datenschutz > Informationen zur Datenverarbeitung, Kapitel 2
- Mehr zum Zugriffsberechtigungskonzept:
  Handbuch > Datenschutz > Downloads
- Mehr zum Rollen-/Rechte-System:
  Handbuch > für Administratoren > Rollen anlegen

### 1.4 Gespeicherte Daten: Wer darf was verwenden?

Der Umfang der Zugriffsbefugnisse richtet sich nach den Aufgaben, die ein DRK-Verband oder eine DRK-Einrichtung aufgrund der jeweiligen Stellung und Funktion im DRK hat.

- Mehr zum Umfang der Zugriffsbefugnisse:
  https://www.drkserver.org/3585/datenschutz > Informationen zur Datenverarbeitung, Kapitel 3

### 1.5 Gespeicherte Daten: Was wird wo aufbewahrt und gelöscht?

Endet Ihre aktive Mitgliedschaft, werden Ihre personenbezogenen Daten durch eine entsprechend autorisierte Person spätestens nach sechs Monaten im aktiven Datenbestand des drk**servers** gesperrt und in das Archiv verschoben. Nach Ablauf der gesetzlichen Aufbewahrungsfristen – hier dient die regelmäßige Verjährungsfrist von drei Jahren zum Jahresende gem. § 195 BGB als Orientierung – werden die Daten endgültig auch aus dem Archivbestand gelöscht.

- Mehr zur Aufbewahrung, Sperrung und Löschung der Daten: https://www.drkserver.org/3585/datenschutz > Informationen zur Datenverarbeitung, Kapitel 5

## 2 Ihre Daten im Gesamtkonzept

### 2.1 Gemeinsame verantwortliche Stelle

Im Rahmen der vertraglichen Vereinbarung haben sich die am drk**server** beteiligten DRK-Landesverbände zur gemeinsamen Datenspeicherung und zum gemeinsamen Betrieb der IT-Infrastruktur verpflichtet. Es erfolgt durch den gemeinsam betriebenen drk**server** eine gemeinsame, zentrale Datenspeicherung, auf die die angeschlossenen DRK-Verbände und DRK-Einrichtungen Einfluss haben. Somit liegt eine gemeinsame verantwortliche Stelle, bestehend aus den DRK-Organisationen, vor. Diese basiert auf EU-Recht.

- Mehr zur gemeinsamen verantwortlichen Stelle: Handbuch > Datenschutz > Gemeinsame verantwortliche Stelle

### 2.2 Umsetzung von IT-Sicherheitsanforderungen

Die EU-Datenschutzgrundverordnung (EU-DSGVO) verlangt die Beachtung mehrerer Punkte zur Umsetzung von Maßnahmen zur IT-Sicherheit.
Im Fall des drk**servers** ist die Umsetzung der IT-Sicherheitsmaßnahmen auf die gemeinsame verantwortliche Stelle (siehe Kapitel 2.1) und auf den beauftragten Dienstleister (Gutzmann GmbH) verteilt. Jede Stelle (vereinfacht: DRK-Gliederung), die am drk**server** angeschlossen ist, muss unter anderem folgende Maßnahmen zur Datensicherheit gewährleisten:

- Zutrittskontrolle: Durch geeignete Maßnahmen muss der Zutritt von Unbefugten unterbunden werden.
  - Beispiel: eine Schlüsselliste
- Zugangskontrolle: Es soll verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
  - Beispiel: Passwortregelung (siehe Kapitel 3.1)
- Zugriffskontrolle: Es soll gewährleistet sein, dass die zur Benutzung Berechtigten ausschließlich Zugriff auf die Daten haben, die sie im Rahmen ihrer Aufgabenstellung benötigen und dass eine unbefugte Verarbeitung, Nutzung oder Speicherung von Daten unterbunden wird.
  - Hiermit ist im Kern das Rollen-/Rechte-Konzept gemeint (siehe Kapitel 1.3)
- Weitergabekontrolle: Es soll verhindert werden, dass Daten während ihres Transportes unbefugt gelesen, verändert oder entfernt werden können.

- Mehr zur Umsetzung von IT-Sicherheitsanforderungen: Handbuch > Datenschutz > Umsetzung von IT-Sicherheitsanforderungen

### 2.3 Datenmissbrauch

Die Datensicherheitsmaßnahmen sollen gewährleisten, dass nur berechtigte Nutzer auf Ihre Daten Zugriff haben. Trotzdem kann es 100%ige Sicherheit nicht geben. Im Fall eines Datenmissbrauchs sind disziplinarische Maßnahmen möglich. Wenn Sie den Verdacht haben, dass Daten missbraucht wurden, sollten Sie sich über ein Formular an den Datenschutzbeauftragten drk**server** wenden. Wer theoretisch wie haften würde, ist im Dokument zur gemeinsamen verantwortlichen Stelle im Kapitel „Gesamt-schuldnerische Haftung“ erläutert.

- Mehr zum Verhalten im Falle von Datenmissbrauch oder dem Verdacht:
  https://www.drkserver.org/3585/datenschutz
  > Informationen zur Datenverarbeitung, Kapitel 4
  > Formular zur Meldung der Verletzung und des Verdachts der Verletzung des Datenschutzes
- Mehr zur gesamtschuldnerischen Haftung:
  Handbuch > Datenschutz > Gemeinsame verantwortliche Stelle

### 2.4 Datenschutzbeauftragter

Seit April 2015 ist Dr. Stefan Drewes der Datenschutzbeauftragte drk**server**. Er ist erreichbar unter datenschutz-drkserver@drk.de.

## 3 So machen Sie Ihre Daten im drkserver sicherer

### 3.1 Passwort

Das Passwort läuft, wenn Sie erweiterte Zugriffsrechte haben, nach 90 Tagen ab und muss dann aktualisiert werden. Es muss verschiedene Anforderungen erfüllen, ist geheim zu halten und darf nicht anderswo notiert werden.
Bei einem mobilen Zugriff muss der verwendete Browser im Privat-Modus genutzt werden. Eine aktuelle Browser-Version sollte verwendet werden. Jedes Mitglied muss darauf achten, dass bei einem mobilen Zugriff keine anderen Personen die Daten sehen können. Daten aus dem drk**server** dürfen nicht lokal gespeichert werden.

- Mehr zum Passwort und zur Datensicherheit:
  https://www.drkserver.org/3585/datenschutz > Merkblatt zur mobilen Nutzung

### 3.2 Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes

Wer Zugang zum drk**server** erhalten möchte, muss unmittelbar nach dem ersten Login mehrere Datenschutzdokumente akzeptieren, darunter die Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes. Danach dürfen Sie personenbezogene Daten nicht unbefugt erheben, verarbeiten oder für andere Zwecke als die mit Ihrer Rolle verknüpften nutzen (siehe hierzu auch Kapitel 1.3). Vertrauliche Informationen dürfen nicht unbefugt verwertet oder weiteren Personen mitgeteilt werden.

- Mehr zu diesem Dokument:
  https://www.drkserver.org/3585/datenschutz > Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes

### 3.3 Dokumente hochladen

In der Mitgliederverwaltung befindet sich unter anderem die Box „Dokumente“. Was hochgeladen werden darf, unterliegt dem Datenschutz. Wählen Sie aus einer entsprechenden Werteliste, beachten Sie aber den Hilfetext („?“-Icon oben rechts in der Box): Keinesfalls dürfen Sie in dieser Box disziplinarische Akten und/oder Vermerke und/oder ärztliche Befunde eintragen. Zu diesen Patientendaten gehören insbesondere Diagnosen, Untersuchung und Therapie einer Krankheit, Arbeitsunfähigkeitsbescheinigungen, Laborbefunde, Röntgenbilder, OP-Berichte und Arztbriefe.
Die Datenschutz-Regelung bezieht sich auch und insbesondere auf den Wertelisteneintrag „Sonstiges“.

- Mehr zu Beschränkungen beim Hochladen von Dokumenten:
  Mitgliederverwaltung > Box „Dokumente“ > Hilfetext

#### 3.3.1 Das Erweiterte Führungszeugnis

Innerhalb der Box „Dokumente“ nimmt das Erweiterte Führungszeugnis eine Sonderrolle ein: Im Rahmen der DRK-Standards zum Schutz vor sexualisierter Gewalt im Verband wird das Einsehen Erweiterter Führungszeugnisse für haupt- und nebenamtlich Tätige als Qualitäts- und Präventionsmerkmal benannt.
Kurz gesagt darf nur dokumentiert werden, ob das Erweiterte Führungszeugnis eingesehen wurde, etwaige Informationen zum Inhalt dürfen nicht gespeichert werden. Und damit natürlich das Zeugnis selbst auch nicht.

- Mehr zum Erweiterten Führungszeugnis:
  www.drkserver.org > Support > Akademie > Erweitertes Führungszeugnis

### 3.4 Datenschutz-Handbuch

Im passwortgeschützten drk**server**-Handbuch finden Sie sämtliche Dokumente zum Datenschutz in verschiedenen Kapiteln. Sie gelangen mit Ihrem drk**server**-Benutzernamen und -Passwort auch in das Datenschutz-Handbuch. Darunter sind auch Informationen zur Einhaltung der EU-Datenschutzgrundverordnung.

- Mehr zum Datenschutz-Handbuch:
  Handbuch > Datenschutz

Sie haben weitere Fragen? Dann wenden Sie sich gerne an das Kompetenzzentrum drk**server** unter support@drkserver.org oder 0251/97 39 600.