

Datenschutzkonzept – Struktur und Inhalte

Vertragliche und organisatorische Rahmenbedingungen

[Die nachfolgenden Stichworte sind nicht als feste Gliederung zu verstehen; sie dienen der Erläuterung und sollen als Fragestellungen – sofern im jeweiligen Kontext zutreffend – bei der Ausformulierung unterstützen.]

- └ Wer ist Auftraggeber? Welche Gesellschaften sind auf Seiten der RKH Gesundheit beteiligt?
- └ Wer ist Hersteller der Software / Auftragnehmer einer Dienstleistung (SaaS)?
- └ Wer ist Ansprechpartner in technischen / datenschutzrechtlichen Belangen bei der RKH?

Darstellung des Zwecks, Inhalts und der Einsatzbereiche der Software / Prozessbeschreibungen

[Die nachfolgenden Stichworte sind nicht als feste Gliederung zu verstehen; sie dienen der Erläuterung und sollen als Fragestellungen – sofern im jeweiligen Kontext zutreffend – bei der Ausformulierung unterstützen.]

- └ Was ist der Auftragsgegenstand? (Softwareprodukt / ggf. Module)
- └ Welche Prozesse sind betroffen? [Bitte Prozessbeschreibungen beifügen]
- └ Welche Kliniken, Fachabteilungen, Zentralbereiche etc. sind betroffen?

Softwarearchitektur

[Die nachfolgenden Stichworte sind nicht als feste Gliederung zu verstehen; sie dienen der Erläuterung und sollen als Fragestellungen – sofern im jeweiligen Kontext zutreffend – bei der Ausformulierung unterstützen.]

- └ Darstellung der Softwarearchitektur / Datenbankstruktur
- └ Wo sind die Daten gespeichert?
- └ Informationen zur Mandantenfähigkeit/-trennung der Software
- └ Welche Schnittstellen gibt es? Welche Exportfunktionen gibt es? (ggf. nähere Beschreibung)

Datensicherheit / Technischer Datenschutz

[Die nachfolgenden Stichworte sind nicht als feste Gliederung zu verstehen; sie dienen der Erläuterung und sollen als Fragestellungen – sofern im jeweiligen Kontext zutreffend – bei der Ausformulierung unterstützen.]

- └ Welche technischen und organisatorischen Maßnahmen (z.B. Verschlüsselung etc.) werden zur Daten-/IT-Sicherheit ergriffen?

Einsatz von Dienstleistern (z.B. Hosting, Support, Wartung etc.)

[Die folgenden Fragen dienen als Hilfestellung zur Darstellung in den Fällen, in denen Daten extern gehostet werden oder in denen aufgrund von (Fern-)Wartung, Support, o.ä. eine Zugriffsmöglichkeit eines/mehrerer Dienstleister/s auf unsere Daten besteht.]

- └ Welche Tätigkeit erbringt der Dienstleister bzw. etwaige Subunternehmer? Welche Zugriffsmöglichkeiten auf die Daten bestehen für den Dienstleister bzw. Subunternehmer?
- └ Gibt es Dienstleister bzw. Subunternehmer und / oder Konzernunternehmen in Drittländern, an die Daten übermittelt werden oder von denen aus eine Zugriffsmöglichkeit auf die Daten besteht?
- └ Bei externem Hosting: Wo sind die Daten gespeichert? Bei mehreren Speicherorten bzw. nur teilweise externem Hosting genaue Darstellung, welche Daten wo gespeichert sind. Wie sind die Übermittlungswege abgesichert? (ggf. Verweis auf Softwarearchitektur) Wie erfolgt die Verschlüsselung und wo ist der Schlüssel gespeichert?
- └ Wer ist unser Ansprechpartner in technischen / datenschutzrechtlichen Belangen beim Auftragnehmer?
- └ Verweis auf abgeschlossenen Auftragsverarbeitungsvertrag

Datenschutzrechtliche Grundlagen

[Die nachfolgenden Stichworte sind nicht als feste Gliederung zu verstehen; sie dienen der Erläuterung und sollen als Fragestellungen – sofern im jeweiligen Kontext zutreffend – bei der Ausformulierung unterstützen.]

- └ Welche Daten werden von welchen Kategorien Betroffener verarbeitet? Zu welchem Zweck?
- └ Welche Rechtsgrundlage/n gibt es?
- └ Sofern eine Einwilligung erforderlich ist: Wie wird diese eingeholt?

Darstellung der Einhaltung der datenschutzrechtlichen Grundsätze

[Die nachfolgenden Stichworte sind nicht als feste Gliederung zu verstehen; sie dienen der Erläuterung und sollen als Fragestellungen – sofern im jeweiligen Kontext zutreffend – bei der Ausformulierung unterstützen. Die nachfolgend eingefügte Tabelle kann, muss aber nicht zur Unterstützung verwendet werden.]

- └ Wie werden die datenschutzrechtlichen Grundsätze eingehalten? Welche Vorkehrungen werden getroffen, insbesondere im Hinblick auf die Grundsätze Rechtmäßigkeit / Zweckbindung; Datenminimierung; Privacy by Design; Privacy by Default?

| Grundsatz | Umsetzung | Bemerkungen |
|---|-----------|-------------|
| Rechtmäßigkeit / Verarbeitung nach Treu und Glauben | | |

| | | |
|---|--|--|
| (Art. 5 Abs. 1 a) DS-GVO) | | |
| Transparenzgebot (Art. 5 Abs. 1 a) DS-GVO) | | |
| Zweckbindung (Art. 5 Abs. 1 b) DS-GVO) | | |
| Datenminimierung (Art. 5 Abs. 1 c) DS-GVO) | | |
| Richtigkeit (Art. 5 Abs. 1 d) DS-GVO) | | |
| Speicherbegrenzung (Art. 5 Abs. 1 e) DS-GVO) | | |
| Integrität und Vertraulichkeit (Art. 5 Abs. 1 f) DS-GVO) | | |
| Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) | | |
| Privacy by design und Privacy by default (Art. 25 DS-GVO) | | |

Darstellung des Rechte-/Rollenkonzepts

[ggf. auch als Anlage beizufügen]

└ Welche Rollen gibt es?

└ Welche Berechtigungen sind eingerichtet? Wer hat auf welche Daten welchen Zugriff?

Darstellung des Protokollierungskonzepts

Dateiname: SO_Gliederung Datenschutzkonzept 03-00_3
 Ersteller: M. Sonntag
 Freigabe: Dr. R. Clement

Seite: 3 von 5
 Erstelldatum: 31.07.2024
 Freigabedatum: 10.09.2024
 Gültig bis: 30.09.2026

[zu beschreiben nur in Bezug auf Logfiles mit Personenbezug]

- └ Welche Logfiles werden gespeichert?
- └ Wer hat auf die Logfiles Zugriff? Wie kann eine Auswertung erfolgen?
- └ Wie lange werden die Logfiles gespeichert?

Darstellung des Löschkonzepts

[ggf. auch als Anlage beizufügen]

- └ Wie wird die erforderliche Löschung der Daten umgesetzt?
- └ Wie kann dem Löschanpruch des Betroffenen begegnet werden?

Sicherstellung Informationspflichten und Auskunftsrechte der Betroffenen

- └ Wie werden die Informationspflichten nach Art. 12 ff. DS-GVO sichergestellt?
- └ Bietet die Software (automatisierte) Möglichkeiten, dem Auskunftsanspruch des Betroffenen nach Art. 15 DS-GVO zu genügen?

Test- / Schulungsdatenbank

- └ Gibt es eine Anonymisierungsfunktion, sofern Bedarf für eine Test-/Schulungsdatenbank gegeben ist?

Datenschutzfolgenabschätzung

- └ ggf. Verweis auf erfolgte Datenschutzfolgenabschätzung bzw. Vermerk über die nicht bestehende Notwendigkeit einer DSFA

Versionshistorie

| Version | Beschreibung | Autor/en | Datum |
|---------|--------------|----------|-------|
| | | | |
| | | | |
| | | | |