Datenschutz-Folgenabschätzung
gemäß Art. 35 DS-GVO

**für** Klicken Sie hier, um Text einzugeben.

**Dokumenten-Historie**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Datum** | **Bearbeiter** | **Bearbeitung** |
| 1.0 | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. | Erstellung/Initialisierung |

# Inhaltsverzeichnis

[1 Stammdaten des Unternehmens/der Organisation 5](#_Toc24265367)

[1.1 Namen und die Kontaktdaten des Verantwortlichen 5](#_Toc24265368)

[1.2 Persönliche Nennung der verantwortlichen Personen 5](#_Toc24265369)

[1.2.1 Geschäftsführung 5](#_Toc24265370)

[1.2.2 Leitung der Datenverarbeitung 5](#_Toc24265371)

[1.2.3 Angaben zur Person des Datenschutzbeauftragten 5](#_Toc24265372)

[2 Beschreibung des Verarbeitungsverfahrens 6](#_Toc24265373)

[2.1 Beurteilung Notwendigkeit hinsichtlich Datenschutz-Folgenabschätzung 6](#_Toc24265374)

[2.2 Darstellung der Einhaltung der grundlegenden datenschutzrechtlichen Prinzipien 6](#_Toc24265375)

[2.2.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz 6](#_Toc24265376)

[2.2.2 Zweckbindung 6](#_Toc24265377)

[2.2.3 Datenminimierung 6](#_Toc24265378)

[2.2.4 Richtigkeit 6](#_Toc24265379)

[2.2.5 Speicherbegrenzung 7](#_Toc24265380)

[2.2.6 Integrität und Vertraulichkeit 7](#_Toc24265381)

[2.2.7 Zusammenfassung 7](#_Toc24265382)

[3 Welche Daten werden verarbeitet? 8](#_Toc24265383)

[3.1 Welche Datenarten werden verarbeitet? 8](#_Toc24265384)

[3.2 Wo werden die Daten erhoben? 9](#_Toc24265385)

[3.3 Darstellung der potenziellen Risiken 10](#_Toc24265386)

[4 Zwecke und Mittel der Verarbeitung 11](#_Toc24265387)

[4.1 Begründung, warum die Informationen verarbeitet werden müssen 11](#_Toc24265388)

[4.2 Darstellung der Notwendigkeit und der Verhältnismäßigkeit der Verarbeitung 12](#_Toc24265389)

[4.3 Darstellung der Erlaubnistatbestände 12](#_Toc24265390)

[4.3.1 Beschäftigtendaten 12](#_Toc24265391)

[4.3.2 Patientendaten 12](#_Toc24265392)

[4.4 Darstellung der Speicherdauer 13](#_Toc24265393)

[4.5 Darstellung der potenziellen Risiken 14](#_Toc24265394)

[5 Weitergabe der Daten 15](#_Toc24265395)

[5.1 Mit wem werden die Daten geteilt? 15](#_Toc24265396)

[5.2 Datenkommunikation mit anderen Systemen 16](#_Toc24265397)

[5.3 Datenübermittlung in Drittstaaten 16](#_Toc24265398)

[5.4 Darstellung der potenziellen Risiken 17](#_Toc24265399)

[6 Wahrung der Betroffenenrechte 18](#_Toc24265400)

[6.1 Transparenzerfordernis 18](#_Toc24265401)

[6.2 Information des Betroffenen 18](#_Toc24265402)

[6.3 Auskunftsrecht 19](#_Toc24265403)

[6.4 Widerspruchsrecht 19](#_Toc24265404)

[6.5 Recht auf Berichtigung und Vervollständigung 19](#_Toc24265405)

[6.6 Recht auf Löschen („Vergessenwerden“) 19](#_Toc24265406)

[6.7 Recht auf Einschränkung der Verarbeitung („Sperrung“) 19](#_Toc24265407)

[6.8 Recht auf Datenübertragbarkeit 20](#_Toc24265408)

[6.9 Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall 20](#_Toc24265409)

[6.10 Fazit 20](#_Toc24265410)

[7 Risikoanalyse, Gewährleistung der Sicherheit der Daten, Darstellung der Auswirkungen der Sicherheitsmaßnahmen auf die Risiken / Restrisikobewertung 21](#_Toc24265411)

[7.1 Risikostufen 21](#_Toc24265412)

[7.2 Festlegung Schutzbedarf 22](#_Toc24265413)

[7.3 Risikominimierung 22](#_Toc24265414)

[7.4 Gewährleistung der Sicherheit der Daten 23](#_Toc24265415)

[7.4.1 Pseudonymisierung personenbezogener Daten 23](#_Toc24265416)

[7.4.2 Verschlüsselung personenbezogener Daten 23](#_Toc24265417)

[7.4.3 Zugriff auf die personenbezogene Daten 24](#_Toc24265418)

[7.4.4 Beschreibung des Verfahrens zur Gewährleistung der Verfügbarkeit der personenbezogenen Daten 24](#_Toc24265419)

[7.4.5 Beschreibung des Verfahrens zur Gewährleistung Zugang zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall, rasch wiederherzustellen 24](#_Toc24265420)

[7.4.6 Beschreibung des Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit von technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung 25](#_Toc24265421)

[7.5 Darstellung der Auswirkungen der Sicherheitsmaßnahmen auf die Risiken, Restrisikobewertung 25](#_Toc24265422)

[8 Begleitende Unterlagen 26](#_Toc24265423)

[9 Fazit 27](#_Toc24265424)

[9.1 Zusammenfassung 27](#_Toc24265425)

[9.2 Bewertung 27](#_Toc24265426)

[9.3 Entscheidung bzgl. Information Aufsichtsbehörde 28](#_Toc24265427)

[9.4 Nächster Prüfungstermin 28](#_Toc24265428)

[Anhang 1: Technisch-Organisatorische Maßnahmen 1](#_Toc24265429)

[1.1 Organisatorische Maßnahmen 1](#_Toc24265430)

[1.1.1 Allgemeine Maßnahmen 1](#_Toc24265431)

[1.1.2 Schulungsmaßnahmen 1](#_Toc24265432)

[1.1.3 Dokumentation 1](#_Toc24265433)

[1.2 Spezielle Technisch-Organisatorische Maßnahmen 2](#_Toc24265434)

[1.2.2 Pseudonymisierung 2](#_Toc24265435)

[1.2.3 Verschlüsselung 2](#_Toc24265436)

[1.2.4 Vertraulichkeit 3](#_Toc24265437)

[1.2.5 Integrität 8](#_Toc24265438)

[1.2.6 Verfügbarkeit 10](#_Toc24265439)

[1.2.7 Belastbarkeit/ Ausfallsicherheit/Wiederherstellbarkeit 11](#_Toc24265440)

[1.3 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung 12](#_Toc24265441)

[1.3.1 Datenschutz-Management 12](#_Toc24265442)

[1.3.2 Incident-Response-Management (IT-Störungsmanagement) 13](#_Toc24265443)

[1.4 Ergänzende Maßnahmen 14](#_Toc24265444)

# Stammdaten des Unternehmens/der Organisation

Die Gesamtverantwortung für den Prozess des Datenschutz-Risikomanagements trägt die Geschäftsführung des Unternehmens.

Es ist organisatorisch sichergestellt, dass es im Bereich DS-Risikomanagement zu keinem Interessens-konflikt kommt und die Unabhängigkeit der Kontroll- und Prüfungsaufgabe gewahrt bleibt, indem

* z. B. eine Trennung zwischen IT und Datenschutz bis hin zur GF besteht
* externe, weisungsunabhängige Prüfstellen eingeschaltet werden
* etc.

Die Geschäftsführung beauftragt persönlich und fachlich geeignete Personen, interne und ggf. externe Stellen mit der Durchführung dieses Prozesses.

## Namen und die Kontaktdaten des Verantwortlichen

|  |  |
| --- | --- |
| Name / Bezeichnung der datenverarbeitenden Stelle | Klicken Sie hier, um Text einzugeben. |
| Straße Hausnummer | Klicken Sie hier, um Text einzugeben. |
| PLZ / Ort | Klicken Sie hier, um Text einzugeben. |
| Telefon | Klicken Sie hier, um Text einzugeben. |
| Telefax | Klicken Sie hier, um Text einzugeben. |
| E-Mail-Adresse | Klicken Sie hier, um Text einzugeben. |
| Internet-Adresse | Klicken Sie hier, um Text einzugeben. |

Angaben zur geschäftlichen Korrespondenz

|  |  |
| --- | --- |
| Rechtsform der Gesellschaft | Klicken Sie hier, um Text einzugeben. |
| Handelsregisternummer | Klicken Sie hier, um Text einzugeben. |
| Umsatzsteueridentifikationsnummer | Klicken Sie hier, um Text einzugeben. |
| Wirtschafts-Identifikationsnummer | Klicken Sie hier, um Text einzugeben. |

## Persönliche Nennung der verantwortlichen Personen

### Geschäftsführung

|  |  |
| --- | --- |
| Vollständiger Name (n) | Klicken Sie hier, um Text einzugeben. |
| Telefon | Klicken Sie hier, um Text einzugeben. |
| Telefax | Klicken Sie hier, um Text einzugeben. |
| E-Mail-Adresse | Klicken Sie hier, um Text einzugeben. |

### Leitung der Datenverarbeitung

|  |  |
| --- | --- |
| Vollständiger Name (n) | Klicken Sie hier, um Text einzugeben. |
| Telefon | Klicken Sie hier, um Text einzugeben. |
| Telefax | Klicken Sie hier, um Text einzugeben. |
| E-Mail-Adresse | Klicken Sie hier, um Text einzugeben. |

### Angaben zur Person des Datenschutzbeauftragten

|  |  |
| --- | --- |
| Vollständiger Name (n) | Klicken Sie hier, um Text einzugeben. |
| Telefon | Klicken Sie hier, um Text einzugeben. |
| Telefax | Klicken Sie hier, um Text einzugeben. |
| E-Mail-Adresse | Klicken Sie hier, um Text einzugeben. |

# Beschreibung des Verarbeitungsverfahrens

Klicken Sie hier, um Text einzugeben.

## Beurteilung Notwendigkeit hinsichtlich Datenschutz-Folgenabschätzung

Hat eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen, ist eine DSFA durchzuführen (Art. 35 DS-GVO).

Weiteres siehe zu dieser DSFA gehörende Excel-Tabelle

## Darstellung der Einhaltung der grundlegenden datenschutzrechtlichen Prinzipien

In Klicken Sie hier, um Text einzugeben. gilt stets der Grundsatz, dass ein Schaden für den Patienten so gut wie möglich ausgeschlossen werden muss, d. h. der Patient bekommt in Klicken Sie hier, um Text einzugeben. die von unserer Seite aus bestmögliche zu erbringende medizinische Versorgung. Daher werden alle Daten dokumentiert, die hierzu erforderlich sein können. Dies erfordert ggf. auch die Verarbeitung von Daten, die nur potentiell zur Behandlung benötigt werden, wie z. B. Allergien.

### Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Die Patientenbehandlung wird im Klicken Sie hier, um Text einzugeben. dokumentiert, so dass die Behandlung bei Bedarf dem Patienten gegenüber nachvollziehbar dargelegt werden kann. Eine entsprechende Protokollierung ermöglicht in Verbindung mit dem Berechtigungskonzept die Darstellung, welche Daten des Patienten von welchem Beschäftigten verarbeitet wurden.

### Zweckbindung

Die Daten werden ausschließlich zu den in Abschnitt 4 dargestellten Zwecken verarbeitet.

### Datenminimierung

Im Rahmen der Patentenbehandlung werden nur notwendige bzw. potentiell notwendige Daten verarbeitet.

### Richtigkeit

Grundlegend für die medizinische Behandlung ist die Korrektheit der erhobenen Daten. Daher ist eine unverzügliche Berichtigung nach Bekanntwerden fehlerhaft gespeicherter Daten unumgänglich und liegt im direkten Interesse sowohl der behandelten Patienten als auch aller im Klicken Sie hier, um Text einzugeben. beschäftigten Personen. Um die Richtigkeit der Daten zu gewährleisten gilt für uns:

* Bei der direkten Erhebung beim Betroffenen oder bei der Erhebung über Bevollmächtigte/Vertreter/Sonstige vertrauen wir auf die Richtigkeit der Daten durch die persönliche Bekanntgabe. Bei Unverständnis fragen wir vor Dokumentation nach.
* Im Bereich der indirekten Erhebung installieren wir Freigabe-Szenarien, um eine Kontrolle auf Korrektheit vorzunehmen.
* Daten von staatlichen Quellen unterliegen einer sensiblen Eigenüberprüfung der Instanzen. Bei Problemen fragen wir bei diesen schriftlich oder telefonisch nach.
* Daten aus öffentlich verfügbaren bzw. nicht-öffentlich verfügbaren Quellen nutzen wir für unsere Systeme nicht.

### Speicherbegrenzung

Die Speicherung richtet sich nach dem Grundsatz der Erforderlichkeit. Neben dem Erfordernis bzgl. der Patientenbehandlung gelten ebenfalls die Erfordernisse den rechtlichen Aufbewahrungspflichten zu genügen, desgleichen im Bedarfsfall die ordnungsgemäße Behandlung nachweisen zu können

### Integrität und Vertraulichkeit

Der Zugriff auf die Daten erfolgt nur nach den im Berechtigungskonzept dargestellten Prinzipien, d. h. es erhalten nur Beschäftigte Zugriff auf die Patientendaten, die diese zur Erfüllung ihrer dienstlichen Pflichten benötigen. Entsprechend dem Backupkonzept erfolgt eine tägliche Sicherung, so dass in Folge eines unbeabsichtigten Verlusts, einer unbeabsichtigten Zerstörung oder unbeabsichtigten Schädigung die Daten wieder hergestellt werden können.

### Zusammenfassung

|  |  |
| --- | --- |
| Die Verarbeitung erfolgt ausschließlich für festgelegte, eindeutige und legitime Zwecke: | [ ]  |
| Die Verarbeitung ist rechtmäßig. | [ ]  |
| Die Datenverarbeitung ist dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt: | [ ]  |
| Eine begrenzte Speicherfrist liegt vor, und zwar | [ ]  |

# Welche Daten werden verarbeitet?

## Welche Datenarten werden verarbeitet?

* Patientendaten
	+ Stammdaten
		- Name/Vorname
		- Geburtsname
		- Geburtsdatum
		- Geburtsort
		- Geschlecht
		- Alter
		- Religionszugehörigkeit
		- Anschrift
		- Kontaktdaten (Telefon, Fax, E-Mail, …)
		- Ethnische Zugehörigkeit
		- Ausbildung
		- Titel
	+ Identifizierende Daten
		- Patient-ID aus Informationssystem
	+ Administrative Daten
		- Versichertenart (privat oder gesetzlich versichert) sowie ggf. Zuzahlungskennzeichen
		- Krankenversicherung/Krankenkasse sowie Versichertenart (Mitglied, Familie usw.)
		- Ggf. Krankenversicherten-Nr. sowie Gültigkeit der Versichertenkarte
		- Klicken Sie hier, um Text einzugeben.
	+ Medizinische Daten
		- Physiologische Auffälligkeiten
		- Klinische Daten aus Anamnese, Diagnose, Therapie
		- Follow-Up-Daten
		- Klicken Sie hier, um Text einzugeben.
* Daten von Anwendern des Systems
	+ Stammdaten
		- Name/Vorname
		- Abteilung
		- Klicken Sie hier, um Text einzugeben.
	+ Identifizierende Daten
		- Nutzer-ID aus des XDS-Informationssystem
	+ Beschäftigtendaten
		- Job-Beschreibung (z. B. Administrator, Oberärztin)
		- Dienstliche Anschrift
		- Dienstliche Kontaktdaten (Telefon, Fax, E-Mail, …)
		- (Fach-) Abteilung
	+ Biometrische Daten (Nur bzgl. Zugang zu Serverräumlichkeiten)
		- Klicken Sie hier, um Text einzugeben.
	+ Im Rahmen Protokollierung
		- User-ID (auch aus Fremd-Systemen
		- IP-Adresse
		- Datum/Uhrzeit von Zugriffen (An-/Abmelden vom System, Zugriff auf bestimmte Daten)

## Wo werden die Daten erhoben?

Die Beschäftigtendaten werden bei Einstellung erhoben und in Klicken Sie hier, um Text einzugeben. eingetragen, wenn ein Vorgesetzter der beschäftigten Person einen Antrag auf Zugriff von Klicken Sie hier, um Text einzugeben. gespeicherten Daten im Rahmen der im Berechtigungskonzept vorgeschriebenen Rahmenbedingungen stellt. Während der Arbeit erfolgt eine Protokollierung aller schreibenden Daten Klicken Sie hier, um Text einzugeben.. Desgleichen wird jeder Zugriff auf Patientendaten protokolliert, der von außerhalb der Behandlungseinheit des Patienten erfolgt. Protokolliert werden (weitere Informationen hierzu finden sich im Protokollierungskonzept):

* User-ID des an- und abmeldenden Anwenders
* Zeitpunkt der An- und Abmeldung
* Änderung und Löschung von Daten
	+ User-ID,
	+ Zeitpunkt,
	+ Klicken Sie hier, um Text einzugeben. -ID des Patienten,
	+ welche Datenarten geändert wurden, z. B. Arztbrief
* Datenexport
	+ User-ID,
	+ Zeitpunkt,
	+ welche Datenarten exportiert wurden, z. B. Arztbrief
* Ausdruck von Patientendaten
	+ User-ID,
	+ Zeitpunkt,
	+ welche Datenarten gedruckt wurden, z. B. Arztbrief
* Notfallanmeldung
	+ User-ID,
	+ Zeitpunkt,
	+ Begründung der Notfallanmeldung)
* Datenverarbeitung im Rahmen einer Notfallanmeldung
	+ User-ID,
	+ Zeitpunkt,
	+ auf welche Datenarten von welchem Patienten wann zugegriffen wurde
* Veränderung am Regelwerk zur Protokollierung
	+ User-ID,
	+ Zeitpunkt,
	+ Begründung der Änderung
* Zugriff auf Protokolldaten
	+ User-ID,
	+ Zeitpunkt,
	+ Begründung der Änderung
* Zugriff mit "Super-User"- / Administrator-Rechten außerhalb der Arbeit an der Systemkonfiguration
	+ User-ID,
	+ Zeitpunkt,
	+ ggf. auf welche Datenarten von welchem Patienten wann zugegriffen wurde

Die Patientenstammdaten werden bei Klicken Sie hier, um Text einzugeben. des Patienten erhoben (entweder direkt beim Patienten oder – im Falle einer Nicht-Ansprechbarkeit – bei Angehörigen oder anderen, den Patienten begleitenden Personen), alle anderen im Rahmen der Patientenbehandlung auftauchenden Daten werden zum Zeitpunkt ihres Anfallens Klicken Sie hier, um Text einzugeben. gespeichert, sofern dies im Behandlungskontext erforderlich ist.

## Darstellung der potenziellen Risiken

Insbesondere den Patientendaten kann ein hohes Risiko bei der unbefugten Kenntnisnahme durch Dritte innewohnen. Für Patienten bestehen insbesondere die folgenden Risiken:

* Diskriminierung, z. B. durch Bekanntwerden ansteckender oder stigmatisierender Erkrankungen
* Finanzieller Verlust, z. B. durch Verlust des Beschäftigungsverhältnisses durch Bekanntwerden einer chronischen Erkrankung, welche z. B. häufige längerfristige krankheitsbedingte Ausfälle im Berufsleben beinhaltet
* Rufschädigung, z. B. durch Bekanntwerden des Vorliegens einer sexuell übertragbaren Erkrankung.

Die genaue Darstellung der Risiken findet sich in der zu dieser DSFA gehörende Excel-Tabelle.

# Zwecke und Mittel der Verarbeitung

## Begründung, warum die Informationen verarbeitet werden müssen

* Patientendaten

Die Behandlung eines Patienten muss nachvollziehbar erfolgen, so dass für den Patienten eine größtmögliche Transparenz bzgl. der medizinischen Behandlung gegeben ist. Zugleich müssen alle medizinischen Daten, die in Folge einer Nach- und/oder Weiterbehandlung erforderlich sein könnten, dokumentiert werden. Weiterhin müssen die Leistungen abgerechnet werden, damit unser Klicken Sie hier, um Text einzugeben. existieren und seine Versorgungsdienstleistung anbieten kann. Daher werden diese Daten Klicken Sie hier, um Text einzugeben. verarbeitet.

Neben der Versorgung des Patienten durch Klicken Sie hier, um Text einzugeben. können die Daten auch noch folgenden Zwecken dienen:

* + Nutzung durch die behandelte Person
		- Selbstversorgung und Pflege der eigenen Gesundheit
		- Häusliche Pflege
		- Information von Familie und/oder interessierten Dritten über die Krankengeschichte (Z. B. Einholung einer Zweitmeinung)
		- Übergabe der Gesundheitsversorgung an einen anderen Erbringer (z. B. zum Zwecke der Nach- oder Weiterbehandlung)
		- Klicken Sie hier, um Text einzugeben.
	+ Gesundheitsversorgung durch Mit- und/oder Nachbehandler
		- Ambulante Versorgung
		- Klinische Versorgung
		- Notfallversorgung
		- Klicken Sie hier, um Text einzugeben.
	+ Forschung
		- Retrospektive Studien
		- Durchführung von Rekrutierungsmaßnahmen für klinische Versuche oder sonstige Forschungsstudien
		- Klicken Sie hier, um Text einzugeben.
* Daten von Anwendern des Systems

Gesundheitsdaten gehören entsprechend den Vorgaben der DS-GVO zu den besonders sensiblen Daten, die einen entsprechend hohen Schutzbedarf aufweisen. Demgemäß dürfen nur Personen Zugriff auf diese Daten bekommen, die ein legitimes Interesse aufweisen können. Daraus folgt die Notwendigkeit der Identifizierung entsprechender Personen.

Weiterhin muss nachvollziehbar sein, sofern Änderungen der Daten erfolgen. Entsprechend werden Änderungen sowohl der Patientendaten selbst als auch der Protokollierungsregeln für Zwecke der aus Art. 5 Abs. 2 DS-GVO resultierenden Rechenschaftspflicht festgehalten.

Daher werden für diese administrative Zwecke folgende Daten verarbeitet:

* + Authentifizierung des Anwenders bzgl. An- und Abmeldung am System
	+ Zuweisung an Zugriffsrechten
	+ Nachverfolgbarkeit wer wann auf welche Daten zugegriffen hat

## Darstellung der Notwendigkeit und der Verhältnismäßigkeit der Verarbeitung

* Beschäftigtendaten

Die User-ID ist zwingend zur Identifikation erforderlich. Da die User-ID nur Klicken Sie hier, um Text einzugeben. bekannt ist, müssen die zur Identifikation der beschäftigten Person erforderlichen Stammdaten ebenfalls Klicken Sie hier, um Text einzugeben. gespeichert werden.

Zur Gewährleistung der Rechenschaftspflicht ist es erforderlich, dass die hierzu relevanten Ereignisse erfasst und dokumentiert werden und hierbei die Zuordnung zu der jeweils das Ereignis auslösenden Person möglich ist. Daher werden sowohl die Ereignisse als auch Zeitpunkt und User-ID protokolliert.

Die Protokolldaten enthalten sensible Informationen, insbesondere über die Beschäftigten. Daher muss ein Zugriff auf die Protokolldaten im Sinne des Schutzes der Beschäftigten gleichermaßen nachvollziehbar sein. Entsprechend erfolgt hierzu eine Protokollierung.

* Patientendaten

Eine Zuordnung der Gesundheitsdaten zum jeweiligen Patienten ist allein schon aus medizinischen Gründen unabdingbar. Daher müssen die Patientenstammdaten Klicken Sie hier, um Text einzugeben. gespeichert werden. Weiterhin ist zur Abrechnung der erbrachten Leistungen erforderlich, dass die hierzu notwendigen administrativen Daten vorliegen.

Im medizinischen Kontext erfolgt die Behandlung immer durch ein Behandlungsteam. Bei der Vielzahl der behandelten Patienten ist eine mündliche Weitergabe der benötigten Daten nicht praktikabel, eine entsprechende Datenmenge könnte kein Mensch im Gedächtnis behalten. Entsprechend ist eine Dokumentation unabdingbar. Um eine schnelle Zugriffsmöglichkeit gewährleisten zu können, ist eine elektronische Dokumentation, die potentiell von jedem Arbeitsplatz des Klicken Sie hier, um Text einzugeben. zeitgleich genutzt werden kann, das Mittel der Wahl. Daneben müssen alle Leistungen elektronisch erfasst werden, die zu Abrechnungszwecken an die jeweiligen Kostenträger übermittelt werden.

## Darstellung der Erlaubnistatbestände

Grundsätzlich regeln die Datenverarbeitung für alle Betroffenen der Art. 6 Abs. 1 DS-GVO, für Beschäftigte im Besonderen der § 26 BDSG-neu sowie für besondere Kategorien von personenbezogenen Daten, z. B. Gesundheitsdaten, der Art. 9 Abs. 2 DS-GVO.

### Beschäftigtendaten

Die Verarbeitung erfolgt im Rahmen der beruflichen Tätigkeit. Erlaubnistatbestand ist daher Art. 6 Abs. 1 lit. b DS-GVO i.V.m. § 26 Abs. 1 BDSG (= Verarbeitung ist für die Erfüllung der aus dem Arbeitsvertrag resultierenden Pflichten des Beschäftigten erforderlich).

### Patientendaten

Die Daten werden zur Patientenbehandlung sowie zur Abrechnung der erbrachten Leistungen benötigt, Erlaubnistatbestand für diese Zwecke ist Art. 9 Abs. 2 lit. h i. V. m. Art. 9 Abs. 3 DS-GVO i. V. m. § 630a ff. BGB sowie § 10 Abs. 1 GDSG NW.

Zur Mit- und Weiterbehandlung werden die hierfür erforderliche Daten an Mit-/Nachbehandler weitergegeben. Rechtsgrundlage hierfür ist Art. 9 Abs. 2 lit. h i. V. m. Art. 9 Abs. 3 DS-GVO sowie § 11 Abs. 1 GDSG NW. Erfolgt die Mit- und Weiterbehandlung durch einen Hausarzt i.S.v. § 73 Abs. 1a SGB V, d.h.

* Allgemeinärzte,
* Kinder- und Jugendärzte,
* Internisten ohne Schwerpunktbezeichnung, die die Teilnahme an der hausärztlichen Versorgung gewählt haben,
* Ärzte mit der Bezeichnung „Praktischer Arzt“, wenn diese auf Grund von landesrechtlichen Vorschriften zur Ausführung des Artikels 30 der Richtlinie 2005/36/EG des Europäischen Parlaments und des Rates vom 7. September 2005 über die Anerkennung von Berufsqualifikationen (ABl. EU Nr. L 255 S. 22, 2007 Nr. L 271 S. 18) bis zum 31. Dezember 1995 erworben wurden,
* Ärzte mit einer Eintragung in das Arztregister für Vertragsärzte, welche auf Grund eines Ausbildungsnachweises über eine inhaltlich mindestens den Anforderungen nach Artikel 28 der Richtlinie 2005/36/EG des Europäischen Parlaments und des Rates vom 7. September 2005 über die Anerkennung von Berufsqualifikationen (ABl. EU Nr. L 255 S. 22, 2007 Nr. L 271 S. 18) entsprechende besondere Ausbildung in der Allgemeinmedizin sind und dieser Ausbildungsnachweis in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder einem Vertragsstaat, dem Deutschland und die Europäische Gemeinschaft oder Deutschland und die Europäische Union vertraglich einen entsprechenden Rechtsanspruch eingeräumt haben, ausgestellt worden ist, erfolgte,
* Ärzte, die am 31. Dezember 2000 an der hausärztlichen Versorgung teilgenommen haben,

so erfolgt die Weitergabe nur bei Vorliegen einer Zustimmung des Patienten gemäß § 73 Abs. 1b SGB V.

Unser Klicken Sie hier, um Text einzugeben. arbeitet an der stetigen Optimierung der Versorgungsqualität. Hierzu ist ein Qualitätsmanagement etabliert und die zur Qualitätssicherung erforderlichen Daten werden auf Grundlage von Art. 9 Abs. 2 lit. i DS-GVO i. V. m. § 299 SGB V i. V. m. § 136 SGB V bzw. den Richtlinien des G-BA verarbeitet.

Im Rahmen der gesetzlichen Pflichten sind wir gezwungen, Daten an gesetzliche Stellen wie Krebsregister zu melden. Rechtsgrundlage hierfür ist Art. 9. Abs. 2 lit. h, i DS-GVO i.V.m. mit dem entsprechenden Meldegesetz.

Weiterhin werden zur Abrechnung die hierfür erforderlichen Daten genutzt. Rechtsgrundlage hierfür ist Art. 9 Abs. 2 lit. f, h DS-GVO i. V. m. z. B. § 301 SGB V sowie § 11 Abs. 1 lit. d GDSG NW.

In seltenen Fällen kann es vorkommen, dass Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen wie beispielsweise der Verteidigung der behandelnden Person vor Gericht oder der Einklagung ausstehender Bezahlungen von erbrachten Leistungen verarbeitet werden müssen. In diesen seltenen Fällen besteht die Rechtgrundlage in Art. 9 Abs. 2. lit. f DS-GVO.

## Darstellung der Speicherdauer

Da die Verarbeitung der Beschäftigtendaten zur Gewährleistung der Rechenschaftspflicht bzgl. der Verarbeitung der Patientendaten erfolgt, richtet sich die Speicherdauer der Beschäftigtendaten nach der Speicherdauer der entsprechenden Patientendaten.

Die Speicherdauer der Patientendaten richtet sich nach den gesetzlichen Vorgaben, d. h. i.d.R. zehn Jahre entsprechend § 630f BGB, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen. Allerdings kann nach einer Risikobewertung eine längere Aufbewahrung von bis zu 30 Jahren (§ 199 Abs. 2 BGB) erfolgen, damit im Falle eines Zivilprozesses die Möglichkeit des Nachweises einer ordnungsgemäßen Behandlung geführt werden kann.

Weitere Informationen finden sich im Archivierungs- sowie im Löschkonzept.

## Darstellung der potenziellen Risiken

Die detaillierte Darstellung der aus den Zwecken und Mitteln der Verarbeitung resultierenden Risiken ist in der zu dieser DSFA gehörenden Excel-Tabelle beschrieben.

# Weitergabe der Daten

## Mit wem werden die Daten geteilt?

|  |  |
| --- | --- |
| Empfänger | Art der Weitergabe |
| Fall-zu-Fall | Vollständige Übermittlung | Direkter Zugriff | Andere (spezifizieren) |
| Innerhalb der Legaleinheit | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. |
| Innerhalb des Konzerns | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. |
| Staatliche Empfänger(spezifizieren) | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. |
| Nicht-staatliche Empfänger(spezifizieren) | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. |

Innerhalb der Legaleinheit

* Klicken Sie hier, um Text einzugeben.

Staatliche Empfänger können z. B. sein:

* Auskünfte an die Polizei/ Staatsanwaltschaft; Rechtsgrundlage ist im Einzelfall zu prüfen, mögliche Erlaubnistatbestände können z. B. in folgenden Vorgaben zu finden sein
	+ § 68 SGB X
	+ § 34 StGB
	+ § 138 StGB
	+ § 16 Abs. 2 MRRG
	+ § 32 BMG
* Gesundheitsamt (meldepflichtigen Erkrankungen entsprechend IfSG)
* Auskünfte an gesetzliche Unfallversicherungen (§§ 199,200, 201, 202, 203 SGB VII)
* Datenaustausch mit den gesetzlichen Krankenkassen (§ 301 SGB V, Landesverträge gemäß § 112 SGB V)
* Pflegekassen (§§ 93, 104, 114, 114a SGB XI)
* Medizinischer Dienst der Krankenkassen sofern öffentlich-rechtlich organisiert (§ 276 Abs. 2 S. 2 SGB V)

Nicht-staatliche Empfänger sind insbesondere:

* Leistungsträger wie z. B. Krankenkassen
* Medizinischen Dienst der Krankenkassen sofern privatrechtlich organisiert (§ 276 Abs. 2 S. 2 SGB V)
* Mit-/nachbehandelnde Ärzte entsprechend § 73 SGB V
* Mit-/nachbetreuende Seelsorger, sofern der Patient dies wünscht
* Mit-/nachbehandelnde ambulante Pflegedienste, sofern der Patient dies wünscht
* Mit-/nachbehandelnde Pflegeheime, sofern der Patient dies wünscht
* Mit-/nachbehandelnder Sozialdienst, sofern der Patient dies wünscht
* Freunde oder Familienangehörige des Patienten, sofern der Patient dies wünscht
* Epidemiologische und klinische Krebsregister entsprechend den gesetzlichen Vorgaben
* Klicken Sie hier, um Text einzugeben.

## Datenkommunikation mit anderen Systemen

Klicken Sie hier, um Text einzugeben.

Die Kommunikation der Systeme ist der nachfolgenden Tabelle 1 zu entnehmen.

| Sender | Was wird gesendet? | HL7-Nachricht | Empfänger |
| --- | --- | --- | --- |
| Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. |

Tabelle : Mit Klicken Sie hier, um Text einzugeben. über Kommunikationsserver verbundene Systeme

## Datenübermittlung in Drittstaaten

Variante 1:

Eine Verarbeitung der Daten in Drittstaaten kommt nur in den folgenden Ausnahmefällen vor:

1. Im Rahmen der Auftragsverarbeitung, wenn Supportleistungen von Dienstleistern aus Drittstaaten zur Aufrechterhaltung der Funktionalität der eingesetzten IT-Systeme zwingend erforderlich ist. Rechtsgrundlage hierfür sind Standardvertragsklauseln (sogenannte „Controller - Processor Vertragsklauseln[[1]](#footnote-1)) gemäß Art. 46 Abs. 2 lit. c DS-GVO.
2. In Ausnahmefällen kann es auf Grund der Weiterentwicklung der medizinischen Versorgung vorkommen, dass Leistungen weltweit nur von wenigen Akteuren erbracht werden. Dies ist z. B. im Rahmen der Bildverarbeitung so, wo einige Verarbeitungsalgorithmen in der ersten Zeit weltweit nur in wenigen Krankenhäusern eingesetzt werden, bevor diese Verarbeitungen überall verfügbar sind. Entscheidet eine Ärztin oder ein Arzt, dass ein derartiges Verfahren für die Behandlung eines Patienten eingesetzt werden sollte (z. B. zur besseren Planung einer erforderlichen Operation), so erfolgt die Verarbeitung im Drittland nach entsprechender Aufklärung des Patienten auf Grund des Erlaubnistatbestandes von Art. 49 Abs. 1 lit. b DS-GVO.
3. In seltenen Fällen, insbesondere bei besonders seltenen Erkrankungen, erfolgt eine gemeinsame Verarbeitung, wobei Partner-Krankenhäuser auch in Drittstaaten existieren. Diese Kooperationen beinhalten sowohl die Konsultationen von Spezialisten der entsprechenden Erkrankungen als auch die Erbringung medizinischer Leistungen wie z. B. Spezialuntersuchungen in Laboren. Diese Mit-Behandlung erfolgt auf Grundlage von Standardvertragsklauseln (sogenannte „Controller - Controller Vertragsklauseln[[2]](#footnote-2)) gemäß Art. 46 Abs. 2 lit. c DS-GVO.

Einige Ärzte veröffentlichen regelmäßig die Ergebnisse ihrer Forschungsarbeit in Fachzeitschriften. Einige Fachzeitschriften verlangen die Veröffentlichung der Rohdaten für die Forschung, damit die Forschungsergebnisse von jedem nachgeprüft werden können, d.h. diese Rohdaten stehen weltweit Fachpersonal zur Verfügung. Bei diesen Rohdaten kann es sich um personenbezogene Daten i.S.v. Art. 4 Abs. 1 DS-GVO handeln, z. B. wenn das Rohmaterial aus Biomaterial besteht, welches die vollständige Gensequenz von Patienten beinhaltet. Hier für existiert keine Rechtsgrundlage. Sollten Ärzte dennoch ohne Einwilligung der Betroffenen entsprechende Veröffentlichungen vornehmen, würden sie gegen die ärztliche Schweigepflicht verstoßen. Eine Veröffentlichung von Forschungsergebnissen mit Personenbezug ohne Einwilligung des Betroffenen wurde daher durch den Verantwortlichen per Dienstanweisung untersagt.

Variante 2:

|  |
| --- |
| **Findet eine Datenübermittlung in Drittstaaten außerhalb der EU statt?** [ ]  Nein[ ]  Ja und zwar: |
| **Abteilungen/Bereiche/Kliniken** | **Art der Daten** | **Zweck /Legitimationsgrundlage**  |
| Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. | Klicken Sie hier, um Text einzugeben. |

## Darstellung der potenziellen Risiken

Die detaillierte Darstellung der aus der Weitergabe der Daten resultierenden Risiken ist in der zu dieser DSFA gehörenden Excel-Tabelle beschrieben.

# Wahrung der Betroffenenrechte

Im Klicken Sie hier, um Text einzugeben. werden neben den Patientendaten auch Beschäftigtendaten gespeichert. Die Beschäftigtendaten dienen der Gewährleistung der gesetzlichen Anforderungen am Betrieb des Klicken Sie hier, um Text einzugeben., z. B. dem Nachweis, wer wann auf welche Patientendaten zu welchem Zeitpunkt zugegriffen hat. Im Nachfolgenden werden daher die Betroffenenrechte aus Sicht der Patienten beschrieben.

Gleichwohl haben selbstverständlich auch Beschäftigte entsprechende Rechte, allerdings werden sie bei der Einstellung auf diese Rechte hingewiesen und erfahren hierbei auch, wie sie diese Rechte wahrnehmen können.

Im Rahmen der Datenschutzschulung erfolgte u. A. eine Schulung des entsprechenden Personals im Umgang mit Betroffenenrechten, so dass eine sach- und fachgerechte Abarbeitung entsprechender Anfragen gewährleistet ist. Zugleich erfahren in diesen Schulungen unsere Beschäftigten ebenfalls, wie sie ihre eigenen Rechte wahrnehmen können.

## Transparenzerfordernis

|  |  |  |
| --- | --- | --- |
| **Transparenz bei Betroffenen durch Erfüllung der Informationspflichten schaffen.** | **Ja** | **Nein** |
| Bedarf die aktuelle Verarbeitungstätigkeit erweiterter Informationspflichten über die bereits etablierten hinweg? **Falls ja, untere Fragen beantworten. Falls nein, Auskunftsende hier.** | [ ]  | [ ]  |
| Gehört die aktuelle Verarbeitungstätigkeit in die Informationspflichten für Beschäftigte? | [ ]  | [ ]  |
| Gehört die aktuelle Verarbeitungstätigkeit in die Informationspflichten für Bewerber? | [ ]  | [ ]  |
| Gehört die aktuelle Verarbeitungstätigkeit in die Informationspflichten für ambulante Patienten? | [ ]  | [ ]  |
| Gehört die aktuelle Verarbeitungstätigkeit in die Informationspflichten für Notfall-/stationäre Patienten? | [ ]  | [ ]  |
| Gehört die aktuelle Verarbeitungstätigkeit in die Informationspflichten für sonstige Betroffene?Wenn ja, welche Betroffenen? Klicken Sie hier, um Text einzugeben. | [ ]  | [ ]  |

## Information des Betroffenen

Bei Klicken Sie hier, um Text einzugeben. erhält jeder Patient eine Information, in welcher die notwendigen Angaben entsprechend Art. 13 resp. Art. 14 DS-GVO enthalten sind.

Auf dieser Information befindet sich auch ein Link auf die Internetseite unseres Klicken Sie hier, um Text einzugeben., welche die von uns beauftragten Auftragsverarbeiter enthält:

* Namen des Auftragsverarbeiters
* die Tätigkeit (z. B. Betreuung IT-System Klicken Sie hier, um Text einzugeben.)
* wann das Vertragsverhältnis begann
* ggfs. wann das Vertragsverhältnis endete (offenes Enddatum = Vertragsverhältnis dauert an).

Sofern die Weitergabe von Daten nicht alle Patienten betrifft wie z. B. die Weitergabe von Daten an ein Krebsregister, wird der betroffene Patient hierüber individuell informiert. Hierzu werden ggf. Formulare der datenempfangenden Stelle genutzt.

Die Informationen werden dabei stets in einer klaren und einfachen Sprache vermittelt, wie es Art. 12 DS-GVO fordert.

## Auskunftsrecht

Die betroffene Person hat das Recht, von uns eine Bestätigung darüber zu verlangen, ob personenbezogene Daten verarbeitet werden. Dies wird ihm im Rahmen der unter Abschnitt 6.2 genannten Information mitgeteilt. In dieser Information wird hierzu sowohl eine Telefonnummer als auch eine spezielle nicht-personalisierte E-Mailadresse, die somit auch bei einem Wechsel des zuständigen Sachbearbeiters erhalten bleibt, genannt.

Unser Klicken Sie hier, um Text einzugeben. gewährleistet die Möglichkeit, dem Patienten die eigenen Daten in einem gängigen, maschinenlesbaren und interoperablen Format (= pdf-Format) zu übergeben, so dass jederzeit die technische Möglichkeit gegeben ist, dem Auskunftsersuchen einer betroffenen Person Folge zu leisten.

## Widerspruchsrecht

Jeder Patient wird auf sein Recht zum Widerspruch gegen eine Datenverarbeitung hingewiesen (Information gemäß Abschnitt 6.2). Zugleich wird der Patient darauf hingewiesen, dass ein Widerspruchsrecht ggf. durch gesetzliche Regelungen eingeschränkt wird, z. B. eine Speicherung aufgrund gesetzlicher Bestimmungen trotz seines Widerspruchs erfolgen muss.

## Recht auf Berichtigung und Vervollständigung

Die betroffene Person hat ein Recht auf Berichtigung und/oder Vervollständigung, sofern die verarbeiteten personenbezogenen Daten, die sie betreffen, unrichtig oder unvollständig sind. Zugleich wird jeder Patient darauf hingewiesen, dass ggf. auch ein Recht auf die Vervollständigung unvollständiger personenbezogener Daten (u. U. auch mittels einer ergänzenden Erklärung) besteht. Beides erfolgt durch die o. g. Information.

Das eingesetzte Klicken Sie hier, um Text einzugeben. ermöglicht die Korrektur fehlerhafter Daten. Im Rahmen der Protokollierung wird den aus § 630f Abs. 1 BGB resultierenden Pflichten genügt.

## Recht auf Löschen („Vergessenwerden“)

Die betroffene Person hat das Recht auf Löschung ihrer personenbezogenen Daten gemäß den Richtlinien nach Art. 17 DS-GVO. Der Patient wird im Rahmen des Informationsschreibens gemäß Abschnitt 6.2 darauf hingewiesen, dass dieses Recht ggf. durch gesetzliche Bestimmungen, z. B. durch die Vorgabe gesetzlicher Aufbewahrungsfristen, eingeschränkt wird.

Das eingesetzte Klicken Sie hier, um Text einzugeben. kann ausschließlich Fallbasiert löschen, d.h. alle Daten eines einzelnen Aufenthaltes eines Patienten.

## Recht auf Einschränkung der Verarbeitung („Sperrung“)

Die betroffene Person hat das Recht, die Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen. Die Voraussetzungen ergeben sich aus Art. 18 DS-GVO.

Der Patient wird im Rahmen des Informationsschreibens gemäß Abschnitt 6.2 darauf hingewiesen, dass dieses Recht ggf. durch gesetzliche Bestimmungen, z. B. durch die Vorgabe gesetzlicher Verarbeitungszwecke wie beispielsweise der Verarbeitung im Rahmen der gesetzlichen Qualitätssicherung entsprechend § 137a SGB V, eingeschränkt wird.

Das eingesetzte Klicken Sie hier, um Text einzugeben. besitzt die Möglichkeit der Sperrung von Zugriffen auf Patientendaten. Für die Entsperrung von Patientendaten ist das Klicken Sie hier, um Text einzugeben. dergestalt konfiguriert, dass eine Entsperrung nur nach Eingabe einer Begründung erfolgen kann. Allerdings besteht keine Möglichkeit zu prüfen, ob vor der Entsperrung eine Unterrichtung der betroffenen Person nach Art. 18 Abs. 3 DS-GVO erfolgte.

## Recht auf Datenübertragbarkeit

Die betroffene Person hat ferner das Recht, ihre personenbezogenen Daten, die sie uns bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Außerdem hat sie das Recht, diese Daten an Dritte zu übermitteln. Ferner hat sie gemäß Art. 20 Abs. 1 DS-GVO das Recht, dass ihre personenbezogenen Daten direkt von uns an einen anderen Verantwortlichen übermittelt werden, soweit dies technisch möglich ist und die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden.

Unser Klicken Sie hier, um Text einzugeben. kann Daten von betroffenen Personen mittels des international im Gesundheitswesen eingesetzten HL7-Standards an andere Informationssysteme weitergeben. Unser Klicken Sie hier, um Text einzugeben. ermöglicht weiterhin Daten in einem gängigen, maschinenlesbaren und interoperablen Format (= pdf-Format) zu exportieren, so dass die Daten in diesem Format übergeben werden können.

## Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall

Die betroffene Person hat jederzeit das Recht, gegen die Verarbeitung ihrer personenbezogenen Daten (die aufgrund von Art. 6 Abs. 1 lit. e oder f erhoben wurden) Widerspruch einzulegen. Dies gilt ebenso für das auf diesen Bestimmungen, sofern zutreffend, geschütztes Profiling. Die Daten werden im Falle eines Widerspruchs nicht weiterverarbeitet, es sei denn, es liegen zwingende schutzwürdige sowie nachweisbare Gründe vor, die den Interessen, Rechten und Freiheiten der betroffenen Person überwiegen, oder der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

## Fazit

[ ]  Die Betroffenenrechte werden seitens des Verantwortlichen gewährleistet.

[ ]  Die Betroffenenrechte werden seitens des Verantwortlichen nur unvollständig berücksichtigt.

[ ]  Die Betroffenenrechte werden seitens des Verantwortlichen nicht berücksichtigt.

# Risikoanalyse, Gewährleistung der Sicherheit der Daten, Darstellung der Auswirkungen der Sicherheitsmaßnahmen auf die Risiken / Restrisikobewertung

## Risikostufen

Die DS-GVO definiert den Begriff „Risiko“ nur indirekt. In Art. 24 Abs. 1 S. 1 DS-GVO findet sich: „Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie **der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken** für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um“. Auch in ErwGr. 75 und 76 werden Risiken als abhängige Größe von der Eintrittswahrscheinlichkeit und der Schwere der Beeinträchtigung der Rechte und Freiheiten der betroffenen Person beschrieben. Daraus folgt, dass die Höhe des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne des Art. 35 DS-GVO somit in Abhängigkeit von „Eintrittswahrscheinlichkeit“ und „Schadensschwere“ darzustellen ist[[3]](#footnote-3).

Die Definition eines Risikos aus Sicht der DS-GVO kann daher lauten:

„Risiko = Produkt aus Eintrittswahrscheinlichkeit und Schwere einer Beeinträchtigung der Rechte und Freiheiten natürlicher von der Verarbeitung betroffener Personen

Nach ErwGr. 76 sollen die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person „in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung“ bestimmt werden. Dabei kennt die DS-GVO verschiedene Grade bzgl. eines Risikos[[4]](#footnote-4):

| **Kategorie** | **Fundort DS-GVO** |
| --- | --- |
| Hohes Risiko / hohen Risiken | ErwGr. 76, 84, 85, 86, 89, 90, 91, 94Art. 34 Abs. 1, Abs. 3(b) und Abs. 4, Art. 35 Abs. 1, Art. 36 Abs. 1, Art. 70 Abs. 1(h) |
| Ernsthaftes Risiko / Erhebliche Risiken | ErwGr. 9, 15, 51 |
| Risiko / Risiken | ErwGr. 28, 38, 39,71, 74, 75, 76, 77, 81, 83, 94, 96, 98, 122Art. 4 Ziff. 22, Art. 4 Abs. 2(g), Art. 24 Abs. 1, Art. 25 Abs. 1, Art. 30 Abs. 5, Art. 32 Abs. 1,2, Art. 33 Abs. 1 |
| Voraussichtlich kein Risiko | Art. 27. Abs. 2(a) |
| Kein Risiko | ErwGr. 80 |

Tabelle : In der DS-GVO verwendete Grade bzgl. eines Risikos für Rechte und Freiheiten von Personen

Daraus lässt sich eine Abstufung bzgl. der Einteilung von Risiken herleiten:

* Hohes Risiko
* Erhebliches Risiko
* (Normales) Risiko
* Voraussichtlich kein Risiko
* Kein Risiko

Das Risiko soll anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung kein Risiko, voraussichtlich kein Risiko, ein normales (im Sinne des „Lebensrisikos“[[5]](#footnote-5)), erhebliches oder ein hohes Risiko in sich birgt.

## Festlegung Schutzbedarf

Gemäß ErwGr. 51 DS-GVO beinhaltet die Verarbeitung der besonderen Kategorien von personenbezogenen Daten, dies sind

* Daten, aus denen die rassische und ethnische Herkunft, hervorgeht,
* Daten bzgl. politischer Meinungen,
* Daten hinsichtlich religiöser oder weltanschaulicher Überzeugungen,
* Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht,
* genetischen Daten,
* biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
* Gesundheitsdaten
* Daten zum Sexualleben oder der sexuellen Orientierung,

immer einen besonderen Schutz verdienen, da „im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können.“. Daraus folgt zweierlei:

1. Es muss bei der Verarbeitung dieser Daten ein „besonderer“ Schutz vorhanden sein; Standardmaßnahmen, wie sie für den Schutz bei der Verarbeitung „normaler“ Daten ausreichen, müssen durch zusätzliche Maßnahmen ergänzt werden, die der Anforderung bzgl. des „besonderen“ Schutzbedarf genügen.
2. In ErwGr. 75 und 76 werden Risiken als abhängige Größe von der Eintrittswahrscheinlichkeit und der Schwere der Beeinträchtigung der Rechte und Freiheiten der betroffenen Person beschrieben Risiken. Die in ErwGr. 51 dargestellten möglichen erheblichen Risiken basieren somit einerseits aus der Schwere der Beeinträchtigung, die einer Verarbeitung dieser besonders sensiblen Daten innewohnt, andererseits aus der Wahrscheinlichkeit, mit welcher die Beeinträchtigung der der Rechte und Freiheiten der betroffenen Personen eintreten *könnte*.

Der in ErwGr. 51 DS-GVO angesprochene „besondere“ Schutz muss also geeignet sein, die Eintrittswahrscheinlichkeit soweit zu reduzieren, dass durch diese Maßnahmen für die Dauer der Verarbeitung **kein** hohes Risiko vorliegt. Andernfalls muss der Verantwortliche, wenn auf die Verarbeitung nach Feststellung des Ergebnisses nicht verzichtet wird, vor Beginn der Verarbeitung gemäß Art. 36 Abs. 1 die zuständige Aufsichtsbehörde konsultieren.

## Risikominimierung

Zur Risikominimierung sind technische (in der Regel IT-bezogene) und organisatorische (z. B. Dienstanweisungen) Maßnahmen zu treffen. Gemäß Art. 32 DS-GVO werden im Anhang „Technische und organisatorische Maßnahmen“ Maßnahmen zur Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit detailliert beschrieben.

## Gewährleistung der Sicherheit der Daten

Die Erfüllung der Anforderungen von Art. 32 DS-GVO wird detailliert in der zu dieser DSFA gehörenden Excel-Tabelle dargestellt. Im Nachfolgenden wird eher ergänzend auf einige Punkte eingegangen.

### Pseudonymisierung personenbezogener Daten

Standardmäßig ist eine Pseudonymisierung im Klicken Sie hier, um Text einzugeben. nicht möglich, ohne hierbei zugleich eine Gefährdung der Gesundheit von Patienten zu riskieren. Durch das Rollen- und Berechtigungskonzept ist gewährleistet, dass auf Patientendaten nur Berechtigte Zugriff haben. Bedingt durch die Notwendigkeit, sich bei der medizinischen Behandlung eines Patienten untereinander zu besprechen, müssen die Patientendaten in identifizierender Form vorliegen.

In wenigen Fällen besonderer Personengruppen, z. B. Personen des öffentlichen Lebens („Very Important Person, VIP“) oder Angestellten unseres Klicken Sie hier, um Text einzugeben. selbst, kann eine Pseudonymisierung trotz der damit verbundenen Risiken, die dies für die jeweilige Person bedeutet, sinnvoll sein. Ob dann eine Pseudonymisierung erfolgt und die damit verbundenen gesundheitlichen Risiken in Kauf genommen werden, wird nach entsprechender Aufklärung in Abstimmung mit der betroffenen Person entschieden.

Für die Testdatenbank, welche für Schulungszwecke eingesetzt wird, wird ein Anonymisierungstool verwendet, welches u. A. die nachfolgen Funktionen hat:

* Anonymisierung von Personendaten wie Vorname, Name, Geburtsdatum etc.
* Anonymisierung von Adressdaten wie Straße, Hausnummer, Postleitzahl, Ort etc.
* Generierung neuer Patientenidentifikatoren (PIDs)
* Generierung neuer Fallnummern
* Umbenennung bzw. Sperrung von Applikationsbenutzern
* Anonymisierung oder Umbenennung von Organisationseinheiten
* Löschen von Schnittstellen- und Auditdaten

### Verschlüsselung personenbezogener Daten

Bei elektronischer Übertragung von Patientendaten an externe Empfänger erfolgt regelmäßig eine Verschlüsselung. Im Rahmen von gesetzlich vorgeschriebenen Übermittlungen sind die rechtlichen Vorgaben bindend.

Bei einem elektronischen Export (z. B. als pdf-Datei) von Patientendaten entscheidet der jeweilige Anwender, ob eine Verschlüsselung erfolgen soll oder nicht, da die Nutzung einer Verschlüsselung nur abhängig von den Möglichkeiten des Empfängers der Daten entschieden werden kann; grundsätzlich wird die Verschlüsselung hierbei empfohlen.

Verbindliche Vorgaben der betroffenen Person werden beachtet.

Bzgl. der Verschlüsselungstechnik können nur die Möglichkeiten unseres Klicken Sie hier, um Text einzugeben. -Herstellers genutzt werden, der sich an den Vorgaben des BSI orientiert[[6]](#footnote-6).

### Zugriff auf die personenbezogene Daten

Der Zugang zu den Daten erfolgt entsprechend der Vorgaben, die in unserem Berechtigungskonzept dargestellt wurden. Grundsätzlich richtet sich der Zugriff auf personenbezogene Daten nach dem „Need-to-know“-Prinzip.

Gegenüber externen Zugriffen ist das Netzwerk durch den Einsatz einer Firewall geschützt. Ein Intrusion Detection System achtet zudem darauf, ob innerhalb unseres Netzwerkes nicht legitimierte Vorgänge erfolgen. Beide Systeme benachrichtigen bei Bedarf das entsprechende Personal, so dass auch von extern nur legitime Zugriffe möglich sind.

Im Berechtigungskonzept ist dargestellt, welche Rechte welcher Rolle zugeteilt werden und wer die jeweilige Entscheidung der Zuteilung von Rollen auf beschäftigte treffen darf.

### Beschreibung des Verfahrens zur Gewährleistung der Verfügbarkeit der personenbezogenen Daten

Näheres siehe Archivierungs- und Backupkonzept, hier erfolgt nur eine kurze Beschreibung zur Darstellung der getroffenen Maßnahmen.

**Einsatz eines Spiegelservers:**

Alle Daten werden auf einen anderen Server „gespiegelt“, d. h. es wird also ein 1:1-Abbild erstellt. Der Spiegelserver steht dabei in einem anderen Brandabschnitt als der eigentliche Server. Die Synchronisierung erfolgt asynchron, daher ist das „Spiegelbild“ nicht immer aktuell. Vielmehr erfolgt die Spiegelung stündlich.

Bei einem Zwischenfall erfolgt hierdurch einerseits nur ein möglichst geringer Datenverlust, andererseits wird der Produktivverlust begrenzt, da seitens der Anwender die Ausfallzeit minimiert wird.

**Backup:**

Ein Sicherungs-System wird zentral bereitgestellt. Dabei erfolgt eine Datensicherung nach dem „Generationenprinzip“. D. h. es wird gewährleistet, dass immer mehrere Sicherungen in verschiedenen zeitlichen Abstufungen („Großvater“, „Vater“ und „Sohn“, daher Generationenprinzip) vorhanden sind, um verschiedene Versionen für eine mögliche Wiederherstellung zur Verfügung zu haben. Die Tagessicherung entspricht dabei dem „Sohn“, die Wochensicherung dem „Vater“ und die Monatssicherung dem „Großvater“

Die Langzeitsicherung erfolgt grundsätzlich auf entsprechenden Bändern oder einem vergleichbaren Sicherungsmedium. Die Lagerung der Bandsicherungen erfolgt in einem anderen Brandabschnitt als dem Standort der Server.

Eine „Rücksicherung wird probehalber quartalsweise für einzelne Datensätze, 1xjährlich für die gesamte Datenbank in einem Testsystem durchgeführt.

### Beschreibung des Verfahrens zur Gewährleistung Zugang zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall, rasch wiederherzustellen

Dies wird durch den Einsatz des Spiegelservers wie auch des Backup-Konzepts gewährleistet

### Beschreibung des Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit von technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Interne Prüfungen der Einhaltung der vorliegend definierten Standards können zu jeder Zeit, auch unangekündigt, durch den Datenschutzbeauftragten bzw. IT-Sicherheitsbeauftragten durchgeführt werden. Grundsätzlich erfolgen interne Prüfungen regelmäßig. Die Ergebnisse einer entsprechenden Prüfung werden dem zuständigen IT Verantwortlichen und dem zuständigen Geschäftsführer in Berichtform übersendet.

Zur Ergänzung interner Prüfaktivitäten können auch externe Prüfungen durch den Verantwortlichen veranlasst werden. Die Vorgehensweise bei externen Prüfungen ist vergleichbar mit dem Vorgehen bei internen.

## Darstellung der Auswirkungen der Sicherheitsmaßnahmen auf die Risiken, Restrisikobewertung

Grundsätzlich stellt jede Verarbeitung von personenbezogenen Daten für die betroffenen Personen ein Risiko bzgl. des Missbrauchs ihrer Daten dar. Bedingt durch die Sensibilität sowohl von Gesundheitsdaten als auch von genetischen Daten, die bei der Patientenbehandlung zwangsläufig verarbeitet werden müssen, ist auch das Risiko für die betroffenen Personen entsprechend hoch.

Daher wurden Maßnahmen getroffen, die das Risiko für betroffene Personen minimieren:

* Ein Berechtigungskonzept beschränkt den berechtigten Zugriff auf die Personen, die entsprechend dem „Need-to-know“-Prinzip Zugriff auf die Daten benötigen
* Pseudonymisierung wird dort eingesetzt, wo es möglich ist.
* Wann immer es angebracht ist, werden Daten verschlüsselt. Eine elektronische Übermittlung erfolgt nur verschlüsselt.
* Sicherheitskonzepte wie der Einsatz eines Spiegelungsservers als auch ein differenziertes Backupkonzept gewährleisten eine Minimierung von Ausfallzeiten und die Wiederherstellbarkeit der Daten.
* Eine Firewall bewacht den Datenverkehr nach extern.
* Ein Intrusion Detection System überwacht den internen Netzbereich auf unerwünschte Vorgänge.
* Regelmäßige Schulungen unserer Beschäftigten zu Fragen bzgl. Datenschutz und IT-Sicherheit gewährleisten eine entsprechende Awareness bei dem bei uns eingesetzten Personal.

Sämtliche Maßnahmen zur Gewährleistung der Sicherheit der Daten wurden dabei stets aus dem Blickwinkel „Safety first“ gewählt. D. h. an erster Stelle steht in unserem Klicken Sie hier, um Text einzugeben. immer die Sicherheit der Patientenversorgung und die Minimierung von Risiken für die Gesundheit unserer Patienten.

Eine detaillierte Darstellung der Maßnahmen sowie der Risikobewertung erfolgt in der zu dieser DSFA gehörenden Excel-Tabelle.

# Begleitende Unterlagen

[ ]  Archivierungskonzept bzw. Archivordnung

[ ]  Berechtigungskonzept

[ ]  Backupkonzept

[ ]  Datenschutzkonzept bzw. Datenschutzrichtlinie

[ ]  IT-Sicherheitskonzept

[ ]  Löschkonzept

[ ]  Notfall-Handbuch

[ ]  Protokollierungskonzept

[ ]  Verfahrensverzeichnis der verantwortlichen Stelle bzw. Verzeichnis von Verarbeitungstätigkeiten

[ ]  Vertrag zur Auftragsverarbeitung mit Klicken Sie hier, um Text einzugeben. -Hersteller

[ ]  Musterdokumente

[ ]  Patienteninformation bzw. Patientenaufklärung bzgl. Betroffenenrechte

[ ]  Patienteneinwilligungen soweit für Verarbeitung im Klicken Sie hier, um Text einzugeben. relevant

# Fazit

## Zusammenfassung

|  |  |
| --- | --- |
| **Die Durchführung der DSFA, einschließlich der Risikoanalyse,** |  |
| * erfolgte korrekt. Die festgelegten Maßnahmen entsprechen im Verhältnis den Risiken der Betroffenen. Die DSFA verlief positiv.
	+ **Empfehlung: Nutzung der Verarbeitungstätigkeit**
 | [ ]  |
| * erfolgte korrekt. Die festgelegten Maßnahmen entsprechen allerdings im Verhältnis **nicht** den Risiken der Betroffenen und sind **nicht** ausreichend. **Eine Nach-Folgenabschätzung und erneute Maßnahmenfestlegung sind notwendig.**
 | [ ]  |
| * erfolgte unter Punkt      unkorrekt. Die festgelegten Maßnahmen entsprechen im Verhältnis den Risiken der Betroffenen und sind ausreichend.

**Eine erneute Betrachtung mit einhergehender Nach-Folgenabschätzung unter Punkt      ist notwendig.** | [ ]  |
| * erfolgte unter Punkt      unkorrekt. Die festgelegten Maßnahmen entsprechen im Verhältnis **nicht** den Risiken der Betroffenen und sind **nicht** ausreichend. Weitere Maßnahmen sind ausgeschlossen. Die DSFA verlief negativ.
	+ **Empfehlung: Meldung Aufsichtsbehörde**
 | [ ]  |

## Bewertung

**Das Gremium der DSFA kommt zu folgendem Ergebnis:**

[ ] Die DSFA, einschließlich Risikoanalyse, verlief **positiv**. Die Verarbeitungstätigkeit geht unter Umsetzung der technisch-organisatorischen Maßnahmen in die Nutzung über.

[ ]  Die DSFA, einschließlich Risikoanalyse, verlief **negativ**. Die Verarbeitungstätigkeit geht nicht in die Nutzung über. Eine Nach-Folgenabschätzung und erneute Maßnahmenfestlegung sind notwendig.

[ ]  Die DSFA, einschließlich Risikoanalyse, verlief **negativ**. Die Verarbeitungstätigkeit geht nicht in die Nutzung über. Eine Nach-Folgenabschätzung und erneute Maßnahmenfestlegung ist nicht möglich.

## Entscheidung bzgl. Information Aufsichtsbehörde

Variante 1

Die Einbeziehung der Aufsichtsbehörde

🞏 ist auf Grund des Ergebnisses der DSFA und der Tatsache, dass die Verarbeitungstätigkeit trotz des Ergebnisses durchgeführt werden soll, notwendig.

🞏 ist nicht notwendig, da die Verarbeitungstätigkeit auf Grund des Ergebnisses der DSFA nicht durchgeführt wird.

⌧ ist nicht notwendig, weil entsprechende Maßnahmen zur Eindämmung
 des Risikos getroffen wurden.

## Nächster Prüfungstermin

Die nächste Prüfung erfolgt alle 3 Jahre bzw. vorher, wenn sich Begleitumstände, die eine erneute DSFA erforderlich erscheinen lassen, ändern.

1. Technisch-Organisatorische Maßnahmen
	1. Organisatorische Maßnahmen

### Allgemeine Maßnahmen

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Personalverwaltungssoftware zur Erfassung der Verpflichtungen aller Beschäftigten[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Es wurde ein Datenschutzbeauftragter benannt und dieser verfügt über angemessene Ressourcen zur Wahrnehmung seiner Aufgabe[ ]  Der Schutzbedarf der Daten wurde festgelegt und die Daten entsprechenden Schutzklassen zugeordnet[ ]  Folgende Verpflichtungen werden bei allen Beschäftigten durchgeführt:[ ]  Verpflichtungen auf das Datengeheimnis[ ]  Verpflichtungen auf die berufliche Schweigepflicht[ ]  Verpflichtungen auf das Fernmeldegeheimnis[ ]  Verpflichtungen auf die Wahrung von Geschäftsgeheimnissen[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

### Schulungsmaßnahmen

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Einsatz einer eLearning-Plattform[ ]  Personalverwaltungssoftware zur Ermittlung, Benachrichtigung und Erfassung der Teilnahme von Datenschutz-Schulungen[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Jeder Mitarbeiter erhält jährlich eine Unterweisung im Datenschutzrecht[ ]  Jeder Mitarbeiter erhält jährlich eine bereichsspezifische Unterweisung bzgl. der Umsetzung datenschutzrechtlicher Anforderungen[ ]  Es werden jährlich Maßnahmen zur Steigerung der Awareness bzgl. Datenschutz durchgeführt[ ]  Es werden jährlich Maßnahmen zur Steigerung der Awareness bzgl. IT-Sicherheit durchgeführt[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

### Dokumentation

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Klicken Sie hier, um Text einzugeben. | [ ]  Es existiert ein Datenschutzkonzept[ ]  Es existiert ein Berechtigungskonzept[ ]  Es existiert ein IT-Sicherheitskonzept[ ]  Es existiert ein Notfall-Handbuch[ ]  Es existiert ein Backupkonzept[ ]  Es existiert ein Archivierungskonzept[ ]  Es existiert ein Löschkonzept[ ]  Es existiert ein Protokollierungskonzept[ ]  Es existiert ein Verzeichnis der Verarbeitungstätigkeiten[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

# Spezielle Technisch-Organisatorische Maßnahmen

### Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Diese zur Zuordenbarkeit erforderlichen zusätzlichen Informationen müssen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, so dass der Verantwortliche keinen Zugriff auf diese Informationen hat.

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Bei einer Pseudonymisierung werden Zuordnungsdaten in einem getrennten und abgesicherten System aufbewahrt, auf welche die pseudonymen Daten verarbeitende Personen keinen Zugriff haben[ ]  Bei einer Pseudonymisierung werden Zuordnungsdaten in verschlüsselt aufbewahrt und die pseudonymen Daten verarbeitende Personen haben keinen Zugriff auf die Schlüssel[ ]  Eine Pseudonymisierung erfolgt immer im jeweiligen Quellsystem[ ]  Eine Prüfung auf Inplausibilitäten und Dopplungen im Vorfeld einer Pseudonymisierung erfolgt grundsätzlich automatisiert[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Es werden alle Daten pseudonymisiert verarbeitet oder es existiert eine Begründung, warum eine pseudonyme Verarbeitung nicht möglich ist[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

### Verschlüsselung

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Automatische Verschlüsselung von Daten, die auf über USB angeschlossene externe Datenträger gespeichert werden[x]  Verschlüsselung von Notebooks[ ]  Verschlüsselung von Tablets[ ]  Verschlüsselung von Smartphones[ ]  Elektronische Signatur von allen E-Mails[ ]  Verschlüsselung von E-Mails, wenn Schlüssel des Empfängers bekannt sind[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Es ist gewährleistet, dass die Erzeugung des Schlüssels bzw. Schlüsselmaterials ein sicherer Prozess ist[ ]  Es ist gewährleistet, dass der Erzeugung des Schlüssels bzw. Schlüsselmaterials eine qualitativ hochwertige Zufallszahlenquelle zugrunde liegt[ ]  Es ist sichergestellt, dass der Salt und/oder der Schlüssel bzw. das Schlüsselmaterial derart erzeugt werden, dass diese weder vorhersagbar sind noch erraten werden können[ ]  Es ist gewährleistet, dass die Vertraulichkeit des Schlüssels bzw. des Schlüsselmaterials während des vollständigen Lebenszyklus der verarbeiteten personenbezogenen Daten gewährleistet ist[ ]  Es ist sichergestellt, dass der Zugriff auf den Salt und/oder den Schlüssel bzw. das Schlüsselmaterial auf ein absolutes Minimum vertrauenswürdiger Anwender beschränkt ist[ ]  Es werden ausschließlich Standard-Verschlüsselungsalgorithmen entsprechend den Empfehlungen anerkannter Organisationen verwendet[ ]  Es ist sichergestellt, dass das verwendete Verfahren eine hinreichende Stärke sowie keinerlei bekannte Schwächen aufweist[ ]  Es ist gewährleistet, dass der Schlüssel geheim gehalten wird[ ]  Es ist sichergestellt, dass ausschließlich Standard-Hash-Funktionen verwendet werden, für die es keine bekannten Schwachstellen gibt[ ]  Es ist sichergestellt, dass bei Verwendung von Hash-Funktionen ein Salt benutzt wird[ ]  Es ist sichergestellt, dass der Salt von ausreichender Qualität ist? (Mindestentropie von 100 Bit)[ ]  Es ist gewährleistet, dass der Salt geheim gehalten wird[ ]  Es liegt ein Konzept zum Schlüsselmanagement vor und dieses enthält Informationen sowohl zum Schlüsseltausch als auch zur Feststellung von Vorgehensweisen bei Kompromittierung[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

### Vertraulichkeit

**Zutrittskontrolle**

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren, schützen personenbezogene Daten vor unbefugtem physischen Zugriff. D.h. unbefugte Personen erhalten keinen physischen Zugriff auf Datenträgern, auf denen personenbezogene Daten gespeichert sind.

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Es erfolgen folgende Zutrittskontrolle für den Zutritt zum Betriebsgelände/Gebäude[ ]  Sicherheitstür(en)[ ]  Magnetkarte[ ]  Chipkarte[ ]  Transponderkarte[ ]  Schlüssel / Manuelles Schließsystem[ ]  Schließsystem mit Codesperre[ ]  Einbruchmeldeanlage[ ]  Brandmeldeanlage[ ]  Videoüberwachung[ ]  Biometrische Verfahren[ ]  Elektronische Signatur[ ]  Andere: Klicken Sie hier, um Text einzugeben.[ ]  Der Zutritt zum Rechenzentrum ist wie folgt gesichert[ ]  Alarmanlagen[ ]  Vergitterte Fenster/Sicherheitsfenster, -schlösser, -türen mit einer definierten Widerstandsklasse[ ]  Lichtschächte[ ]  Lüftungsöffnungen[ ]  Rollos gegen Hochschieben gesichert[ ]  Feuerleiter[ ]  Bewegungsmelder[ ]  Andere:[ ]  Die Server befinden sich in abschließbaren Serverschränken[ ]  Gelagerte Notebooks befinden sich unter Verschluss in gesicherten Räumen[ ]  Die Aufbewahrung von Datensicherungen (z. B. Bänder, CDs) erfolgt in zutrittsgeschützten Safes oder Räumen[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Es existiert ein Zutrittskontrollsystem, in welchem die zutrittsberechtigten Mitarbeiter festgelegt sind[ ]  Es erfolgen folgende Zutrittskontrolle für den Zutritt zum Betriebsgelände/Gebäude[ ]  Empfang / Rezeption / Pförtner[ ]  Besucherbuch / Protokoll der Besucher[ ]  Verschließen von Türen und Fenstern, sobald Personal nicht im Raum[ ]  Mitarbeiterausweise[ ]  Besucherausweise[ ]  Werkschutz/Wachpersonal[ ]  Andere: Klicken Sie hier, um Text einzugeben.[ ]  Es bestehen Regelungen für den Zutritt von Fremdpersonal, Reinigungspersonal, Besucher[ ]  Die Begleitung von Gästen im Gebäude ist in einer Richtlinie geregelt[ ]  Differenzierte Sicherheitsbereiche/-zonen (z. B. für Server, Großrechner, Archiv) sind festgelegt[ ]  Die Datenträger sind Bestandteil des Zutrittsschutzkonzepts[ ]  Es liegt eine Anweisung zur Ausgabe von Schlüsseln vor[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

**Zugangskontrolle**

Maßnahmen zur Zugangskontrolle dienen der Verhinderung der unbefugten Nutzung von Anlagen/Systemen, mit welchen (personenbezogene) Daten verarbeitet werden.

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Die unbefugte Nutzung von IT-Systemen wird wie folgt verhindert[ ]  User-ID[ ]  Benutzername/Passwort[ ]  Biometrische Kontrolle[ ]  Automatische Bildschirmsperre mit Passwortaktivierung[ ]  Sperrung des Kontos nach 3-maligen Fehlversuchen, erneute Anmeldung erst nach 10 Minuten möglich[ ]  Vollständige Sperrung des Kontos nach 3aufeinanderfolgenden Fehlversuchen mit kurzfristiger Kontensperrung[ ]  Sonstige: Klicken Sie hier, um Text einzugeben.[ ]  Zwei-Faktor-Authentifizierung, die zwei Faktoren sind[ ]  Benutzername/Passwort (statisch)[ ]  Einmal Passwort / Hardware Token[ ]  Einmal Passwort / Mobiltelefon[ ]  PKI / zertifikatsbasierte Anmeldung[ ]  SMS Passwort[ ]  Sicherheitsfragen[ ]  Geo-Lokalisation[ ]  Verhaltensbasierend[ ]  Geräte-Identifikation[ ]  Virtuelle Smartcards[ ]  Anderer Faktor: Klicken Sie hier, um Text einzugeben.[ ]  Passwörter werden ausschließlich verschlüsselt gespeichert[ ]  Es existiert ein Mobile-Device-Management-System[ ]  Über alle Aktivitäten in den IT-Systemen werden automatisch Protokolle erstellt[ ]  Die Nutzung von IT-Systemen mithilfe von Einrichtungen der Datenübertragung durch Unbefugte wird durch folgende Maßnahmen verhindert oder zumindest nachvollziehbar gemacht:[ ]  Standleitung[ ]  Wählleitung mit automatischem Rückruf[ ]  Teilnehmerkennung[ ]  Ausweisleser[ ]  Protokollierung der Systemnutzung und Protokollauswertung[ ]  Sonstige:[ ]  Automatische Aktivierung eines Sperrbildschirms, wo dies den Arbeitsablauf nicht unzulässig behindert[ ]  Sperrung/Deaktivierung von nicht benötigten USB-Ports[ ]  Sperrung/Deaktivierung von nicht benötigten Bluetooth-Schnittstellen[ ]  Sperrung/Deaktivierung von nicht benötigten WLAN-Schnittstellen[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Es existiert eine Benutzerverwaltung, in welcher Benutzern Authentifizierungsmöglichkeiten zugewiesen werden[ ]  Es gibt eine Richtlinie zur Vergabe und Nutzung von Passwörtern[ ]  Jeder Berechtigte verfügt über ein eigenes nur ihm bekanntes Passwort[ ]  Es existiert ein Mobile-Device-Richtlinie, in welcher der Umgang mit mobilen Geräten festgelegt ist[ ]  Neue Schwachstellen in den IT-Systemen werden nach Bekanntwerden gemeldet, analysiert und ggf. behoben, um das Eindringen seitens unbefugter Dritter in die IT-Systeme zu verhindern[ ]  Es gibt definierte und erprobte/wirksame Verfahren für die Fachabteilungen und Technik im Fall eines (erfolgten) externen Angriffs auf relevante Daten und Systeme[ ]  IT-Systeme werden auf die Wirksamkeit (Effektivität) eingesetzter Maßnahmen gegen das Eindringen seitens unbefugter Dritter getestet[ ]  Penetrationstests erfolgen[ ]  Jährlich[ ]  Alle 2 Jahre[ ]  Alle Klicken Sie hier, um Text einzugeben. Jahre[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

**Zugriffskontrolle**

Hierunter fallen Maßnahmen, welche dafür Sorge tragen sollen, dass die zur Benutzung eines Informationssystems Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und eine unberechtigte Verarbeitung verhindert wird.

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Discretionary Access Control (DAC)[ ]  Mandatory Access Control (MAC)[ ]  Type Enforcement (TE)[ ]  Multi-Level Security (MLS)[ ]  Role Based Access Control (RBAC)[ ]  Attribute-based access control (ABAC)[ ]  Context-Based Access Control (CBAC)[ ]  Media Access Control[ ]  Es liegt eine eindeutige Zuordnung zwischen jedem Datenträger (Laufwerk etc.) und Berechtigten vor (insb. bei Gruppenlaufwerken)[ ]  Die Programm- und Dateibenutzung wird protokolliert und stichprobenartig ausgewertet[ ]  Werden sog. „Superuser“ Accounts eingesetzt, so erfolgt ein Monitoring sowie eine regelmäßige Kontrolle von Aktivitäten, die mithilfe dieser Benutzerkonten durchgeführt werden[ ]  Andere: Klicken Sie hier, um Text einzugeben. | [ ]  Es besteht ein dokumentiertes Berechtigungsmanagement (Berechtigungskonzept), in dem verbindlich geregelt ist, wie Berechtigungen beantragt, freigegeben, umgesetzt und wieder entzogen werden[ ]  Für jedes eingesetzte Datenbanksystem ist im Berechtigungssystem die Rechte an Datenbanktransaktionen festgehalten[ ]  Im Rahmen dieses Berechtigungsmanagements ist manipulationssicher nachweisbar, wer wann welche Berechtigungen innehatte[ ]  Es bestehen differenzierte Berechtigungen (z. B. für Lesen, Löschen, Ändern)[ ]  Es bestehen differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem[ ]  Es besteht eine funktionelle/personelle Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (techn.)[ ]  Es existiert eine Benutzerverwaltung, über die Berechtigungen verwaltet werden[ ]  Es liegt ein Konzept der Laufwerksnutzung und -zuordnung vor[ ]  Die Wiederherstellung von Daten aus Backups ist in einem verbindlichen Verfahren geregelt (wer darf wann auf wessen Anforderung Backup-Daten einspielen?)[ ]  Es erfolgt bei einer evtl. Programmentwicklung eine Funktionstrennung zwischen Test- und Produktionsumgebung[ ]  Andere: Klicken Sie hier, um Text einzugeben. |

**Weitergabekontrolle**

Hierbei handelt es sich um Maßnahmen, die verhindern, dass Daten unbefugt weitergegeben werden. Insbesondere soll verhindert werden, dass Daten bei einer elektronischen Übertragung bzw. Transport nicht unbefugt verarbeitet werden können.

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Es erfolgt eine Legitimationsprüfung der Berechtigten[ ]  Folgende Versendungsart(en) personenbezogener Daten besteht/bestehen[ ]  Datenträgertransport (z. B. Post, zuverlässiger Boten/Kurier)[ ]  Verpackungs- und Versandanschrift[ ]  Transportbegleitung und geschlossene Behältnisse[ ]  Datenverschlüsselung[ ]  E-Mail, [ ]  FTP[ ]  SSH[ ]  VPN (Verschlüsselung)[ ]  Sicheres Web-Formular / -Portal[ ]  Gesicherte/Verschlüsselte Datenleitung[ ]  § 301 FTAM over IP[ ]  Sektorenübergreifende Qualitätssicherung nach Sektorenübergreifende Qualitätssicherung[ ]  Die Daten werden beim Transport nicht zwischengelagert[ ]  Der Versand bzw. Transport der Datenträger wird dokumentiert (z. B. Protokoll wer wann welche Informationen erhalten hat)[ ]  Eingang und Ausgang der Datenträger lückenlos dokumentiert[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Für Übermittlung/Transport der Daten sind Befugte festgelegt[ ]  Es ist sichergestellt, dass Transportdienstleister sorgfältig in Hinblick auf Zuverlässigkeit und Sicherheit beim Transport ausgewählt werden[ ]  Es ist sichergestellt, dass die Transportbehälter gesichert sind und nur von den berechtigten Stellen geöffnet werden[ ]  Folgende ergänzende Maßnahmen sind für Übermittlung/Transport von Daten festgelegt[ ]  Entgegennahme und Rückmeldung[ ]  Vollständigkeitsprüfung[ ]  Richtigkeitsprüfung[ ]  Protokollierung (z. B. Datenträger-Begleitzettel)[ ]  Betroffene Mitarbeiter sind darüber informiert, wie Datenträger zu transportieren sind[ ]  Es ist geregelt, was passieren muss, wenn beim Datenträgertransport Fehler (z. B. Verlust von Datenträgern) auftreten[ ]  Es ist geregelt, wer in welcher Art und Weise Zugang zu/Zugriff auf diese Eingangs-/Ausgangs- und Versandprotokolle hat[ ]  Es existiert eine Übersicht über alle regelmäßigen elektronischen Übertragungen[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

**Trennungskontrolle**

Hierbei handelt es sich um Maßnahmen, welche gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies kann beispielsweise durch logische oder physikalische Trennung der Daten erreicht werden.

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Die Daten verschiedener Mandanten werden physisch getrennt verarbeitet[ ]  Die Daten verschiedener Mandanten werden logisch getrennt verarbeitet[ ]  Die Datensicherungen verschiedener Mandanten erfolgen auf separaten Datenträgern[ ]  Es existiert eine Trennung zwischen Test- und Produktivdaten[ ]  Sandboxing[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Die Daten anderer Mandanten werden von unterschiedlichen Mitarbeitern beim Auftragnehmer verarbeitet, so dass die Gefahr der Weitergabe von Geschäftsgeheimnissen minimiert wird[ ]  Es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung der Daten anderer Mandanten Rechnung trägt[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

**Zweckbindung**

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Es werden nur solche Daten verarbeitet, die unmittelbar dem eigentlichen Zweck dienen und die zur Erfüllung der Aufgabe oder Durchführung des Prozesses notwendig sind[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

### Integrität

**Eingabekontrolle**

Diese Maßnahmen sollen dafür sorgen, dass man nachträglich feststellen kann, ob und wenn ja von wem personenbezogene Daten in informationstechnischen Systemen eingegeben, verändert oder entfernt worden sind.

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Es wird maschinell protokolliert, wer was wann in der fachlichen Anwendung eingegeben hat[ ]  Es wird maschinell protokolliert, wer was wann in der fachlichen Anwendung geändert hat[ ]  Es wird maschinell protokolliert, wer was wann in der fachlichen Anwendung gelöscht hat[ ]  Es erfolgt eine Protokollierung der Administratorentätigkeiten insbesondere von Anlegen von Benutzern, sowie des Änderns von Benutzerrechten[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Es existiert eine Übersicht, welche IT-Systeme die Erfassung personenbezogener Daten ermöglichen[ ]  Es sind Benutzerberechtigungen festgelegt und diese sind wie folgt differenziert[ ]  Lesen[ ]  Ändern[ ]  Löschen[ ]  Teilzugriff auf Daten bzw. Funktionen[ ]  Feldzugriff bei Datenbanken[ ]  Andere:[ ]  Es sind gesetzlich bestimmte (HGB u. A.) oder unternehmenseigene Aufbewahrungsfristen festgelegt[ ]  Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden[ ]  Es existiert ein Archivierungskonzept in welchem festgelegt ist, welche Daten wie lange aufzubewahren sind und wer unter welchem Umständen Zugriff auf archivierte Daten erhalten darf bzw. muss[ ]  Es existiert ein Löschkonzept. In welchem festgelegt ist, wer welche Daten zu welchen Zeitpunkten auf welche Weise löschen darf bzw. muss[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

**Auftragskontrolle**

Hierunter fallen Maßnahmen, welche gewährleisten, dass im Auftrag verarbeitete personenbezogene Daten nur entsprechend der Weisungen des Auftraggebers verarbeitet werden.

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Es existiert eine Dokumentation, welche die lückenlose Nachvollziehbarkeit der einzelnen im Rahmen der Auftragsausführung erforderlichen Arbeitsschritte gewährleistet[ ]  Es erfolgen regelmäßig Audits bei Dienstleistern[ ]  Jährlich[ ]  Alle 2 Jahre[ ]  Alle \_\_\_ Jahre[ ]  Es werden automatisch Nachweise bzgl. der Sicherheit der Verarbeitung (Art. 32 DS-GVO) bei Dienstleistern angefordert[ ]  Jährlich[ ]  Alle 2 Jahre[ ]  Alle[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Auftragsverarbeiter werden ausschließlich nach einer Überprüfung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt[ ]  Es werden nur Auftragsverarbeiter ausgewählt, die einen qualifizierten Datenschutzbeauftragten benannt haben und bei denen der Datenschutzbeauftragte über angemessene Ressourcen zur Wahrnehmung seiner Aufgabe verfügt[ ]  Es existiert ein Vertrag zur Auftragsverarbeitung, der den Anforderungen der DS-GVO genügt[ ]  Im Vertrag zur Auftragsverarbeitung wird jeder Auftragsverarbeiter vertraglich verpflichtet, dass diese allen seinen Beschäftigten dieselben Geheimhaltungsverpflichtungen auferlegen, die auch für die Beschäftigten des Klicken Sie hier, um Text einzugeben. gelten[ ]  Es wurde überprüft, dass der Auftragsverarbeiter ein Verzeichnis der Auftrags-Verarbeitungstätigkeiten führt[ ]  Die Leistungsbeschreibung spezifiziert explizit die zulässigen Arbeiten[ ]  Die weisungsbefugten Personen auf Seite des Auftraggebers sind benannt und beim Auftragnehmer bekannt[ ]  Die zur Entgegennahme und Ausführung von Weisungen des Auftraggebers beim Auftragnehmer befugten Personen sind benannt[ ]  Alle Weisungen des Auftraggebers an den Auftragnehmer erfolgen schriftlich[ ]  Mitarbeiter des Auftragnehmers erhalten folgende schriftliche Datenschutz-Informationen[ ]  Merkblatt[ ]  Gesetzestext[ ]  Kopie der Verpflichtungserklärung[ ]  Andere:[ ]  Wenn der Auftragnehmer einen Unterauftragnehmer zur Erfüllung der Auftragsverarbeitung einsetzt, ist gewährleistet[ ]  Der Auftragnehmer informiert den Auftraggeber über alle eingesetzten Unterauftragnehmer, die Daten des Auftraggebers verarbeiten[ ]  Mit Unterauftragnehmern werden Auftragsverarbeitungsverträge abgeschlossen und die Verträge des Auftragnehmers mit dem Unterauftragnehmern spiegeln die Anforderungen des Auftraggebers an den Auftragnehmer wider[ ]  Mit Unterauftragnehmern werden Datenschutzvereinbarungen abgeschlossen, die alle Geheimhaltungsvereinbarungen enthalten, die auch für die Beschäftigten des Auftraggebers gelten[ ]  Erfolgt ein Verarbeitung durch den Auftragsverarbeiter oder durch Unterauftragnehmer außerhalb der EU, so wird ein angemessenes Datenschutzniveau gewährleistet durch[ ]  EU-Standard-Vertragsklauseln[ ]  Verarbeitung in Drittländer mit einem durch die EU-Kommission festgestelltem angemessenem Datenschutzniveau[ ]  Privacy-Shield-Vereinbarung[ ]  Individualvertrag mit Genehmigung durch die Aufsichtsbehörden[ ]  Anderes: Klicken Sie hier, um Text einzugeben.[ ]  Die meldepflichtigen Vorfälle sind spezifiziert und sowohl den eigenen beschäftigten als auch allen vom Auftragnehmer eingesetzten Personen bekannt, inkl. Personen von ggf. existierenden Unterauftragnehmern[ ]  Auf Anforderung kann belegt werden, dass der jeweilige Auftrag strikt nach den Weisungen des Auftraggebers durchgeführt wurde[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

### Verfügbarkeit

Hierunter fallen Maßnahmen, welche dafür sorgen sollen, dass personenbezogene Daten gegen zufällige Zerstörung oder zufälligen Verlust geschützt sind.

**Backup- und Recoverykonzept**

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Es existiert ein Brandschutz, insbesondere Feuer- und Rauchmeldeanlagen[ ]  Im Serverraum ist ein Feuerlöscher verfügbar[ ]  Der Serverraum ist klimatisiert[ ]  Im Serverraum erfolgt eine Überwachung von Temperatur und Feuchtigkeit[ ]  Jeder Server ist mit einer unterbrechungsfreien Stromversorgung (USV) verbunden[ ]  Ausgesuchte Clients, insbesondere Clients von Administratoren, sind mit unterbrechungsfreien Stromversorgung (USV) verbunden[ ]  Es werden Hardware-RAID-Systeme eingesetzt[ ]  Im Serverraum sind Schutzsteckdosenleisten im Einsatz[ ]  Der Serverraum wird mit einer Videoanlage überwacht[ ]  Es existiert eine Alarmanlage, welche ein unbefugtes Eindringen in den Serverraum meldet[ ]  Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.) ist vorhanden[ ]  Backups werden regelmäßig auf Datenvollständigkeit kontrolliert[ ]  Die Sicherung bezieht auch Notebooks und nicht vernetzte Systeme mit ein[ ]  Es wird regelmäßig überprüft, ob eine Rekonstruktion der gesicherten Daten tatsächlich möglich ist[ ]  Alte oder unbrauchbare Datenträger werden datenschutzrechtlich ordnungsgemäß vernichtet[ ]  Es erfolgt eine Festplattenspiegelung[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Es existiert ein angemessenes Backup- und Recoverykonzept[ ]  Es ist festgelegt, welche Daten für welchen Zeitraum gesichert werden und die anschließende Löschung der Daten ist gewährleistet[ ]  Das „Haltbarkeitsdatum“ der Sicherungsbänder wird beachtet[ ]  Es gibt eine Vereinbarung bzgl. Übergabe der (Daten-)Sicherungen[ ]  Eine katastrophensichere Aufbewahrung der Datenträger ist sichergestellt[ ]  Backups werden (auch) geografisch an von den Servern unterschiedliche Speicherorte aufbewahrt[ ]  Keine sanitären Anschlüsse im oder oberhalb des Serverraums[ ]  Es existiert ein Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung (BCM-Konzept)[ ]  Es existiert ein Notfallhandbuch mit Notfallplänen, Darstellung der Notfallorganisation – klare Regelung der Verantwortlichkeiten im Notfall[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

### Belastbarkeit/ Ausfallsicherheit/Wiederherstellbarkeit

Hierunter fallen Maßnahmen, welche dafür sorgen sollen, dass personenbezogene Daten bei Verlust oder Zerstörung schnell wiederhergestellt werden können.

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Es existiert ein Netzwerk-Monitoring, welches alle relevanten Server, Dienste und Prozesse überwacht und Abweichungen zuverlässig meldet[ ]  Es existiert eine redundante Benachrichtigungsfunktion (z. B. Mail, SMS), welche über Störungen/Ausfälle relevanter IT-Systeme informiert[ ]  Es gibt eine unterbrechungsfreie Stromversorgung[ ]  Es werden Hardware-RAID-Systeme eingesetzt[ ]  Server sind mit redundanter Hardware (Netzteil, Netzwerkkarte, usw.) ausgestattet?[ ]  Es sind Ausweich-Rechenzentren vorhanden (Hot- bzw. Cold Stand-by)[ ]  Es übernehmen redundante Stand-By-Systeme bei Ausfällen wechselseitig die Prozesse[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Es wurden Single-Points-of Failure identifiziert und durch angemessene Maßnahmen behandelt[ ]  Es wurden alle Konfigurationsparameter der benutzten Betriebssysteme und Anwendungen sowie der eingesetzten Protokolle dokumentiert[ ]  Es wurden die maximalen Ausfallzeiten für die verschiedenen IT-Systeme (Client, Fileserver, Datenbankserver, usw.) festgelegt[ ]  Die zu erreichende Verfügbarkeit für die verschiedenen IT-Systeme (Client, Fileserver, Datenbankserver, usw.) wurde festgelegt[ ]  Es wurde festgelegt, welche Person bei welcher Störung oder welchem Ausfall zu benachrichtigen ist[ ]  Es existiert ein Notfallplan mit Regelungen wie beispielsweise * Wohin können Anwendungen ggf. hin verlagert werden
* Welche Server können/müssen ggf. geordnet heruntergefahren werden

[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

**Server- und Client-Absicherung**

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Es existiert für jeden Client ein passendes Image, so dass bei Bedarf der Client jederzeit wiederhergestellt werden kann[ ]  Es gibt Reserve-Clients (PC, Laptop, Tablet, Smartphone, …), so dass bei einem Ausfall der Client ausgetauscht und die Arbeit schnellstmöglich wieder aufgenommen werden kann[ ]  Folgende Sicherheitssysteme schützen Soft- und/oder Hardware vor Angriffen[ ]  Virenscanner[ ]  Firewalls[ ]  Spamfilter[ ]  Verschlüsselungsprogramme[ ]  Intrusion-Detection-System[ ]  Intrusion-Prevention-System[ ]  Andere: Klicken Sie hier, um Text einzugeben.[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

# Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

### Datenschutz-Management

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Datenschutz-Management-IT-System im Einsatz[ ]  Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Beschäftigte nach Bedarf / Berechtigung[ ]  Intranet[ ]  Wiki[ ]  Interne Social Media Platform wie bspw. Blog[ ]  Eine Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen wird regelmäßig durchgeführt[ ]  Halbjährlich[ ]  Jährlich[ ]  Alle zwei Jahre[ ]  Alle Klicken Sie hier, um Text einzugeben. Jahre[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Verantwortlichkeiten sind eindeutig zugewiesen[ ]  Rechenschaftspflicht (Nachweis über Einhaltung datenschutzrechtlicher Vorgaben)[ ]  Benannter Datenschutzbeauftragter[ ]  Extern[ ]  Intern[ ]  Beschäftigte geschult und auf Vertraulichkeit/Geheimhaltung verpflichtet[ ]  Regelmäßige Sensibilisierung der Mitarbeiter[ ]  Datenschutz durch Technikgestaltung („Privacy by Design) wird bei allen Verarbeitungsprozessen umgesetzt[ ]  Datenschutz durch datenschutzfreundliche Voreinstellungen („Privacy by Default) wird bei allen Verarbeitungsprozessen umgesetzt[ ]  Datenschutz-Folgenabschätzung wird bei Bedarf durchgeführt[ ]  Betroffenenrechte werden gewährleistet[ ]  Verzeichnis von Verarbeitungstätigkeiten existiert und ist auf dem jeweils aktuellen Stand[ ]  Dokumentation aller Verletzungen des Schutzes personenbezogener Daten[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

### Incident-Response-Management (IT-Störungsmanagement)

| Technische Maßnahmen | Organisatorische Maßnahmen |
| --- | --- |
| [ ]  Es existiert ein Netzwerk-Monitoring, welches alle relevanten Server, Dienste und Prozesse überwacht und Abweichungen zuverlässig meldet[ ]  Intrusion-Detection-System[ ]  Intrusion-Prevention-System[ ]  Anderes: Klicken Sie hier, um Text einzugeben. | [ ]  Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)[ ]  Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen[ ]  Team zum Umgang mit Sicherheitsvorfällen gebildet und Team beinhaltet[ ]  Mitglied der Geschäftsführung[ ]  IT-Leiter[ ]  Datenschutzbeauftragter[ ]  IT-Sicherheitsbeauftragter[ ]  Mitglied der Pressestelle/Öffentlichkeitsarbeit[ ]  Im Vorfall involvierte Personen[ ]  Dokumentation von Sicherheitsvorfällen und Datenpannen[ ]  Formaler Prozess zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen beschrieben und etabliert[ ]  Anderes: Klicken Sie hier, um Text einzugeben. |

# Ergänzende Maßnahmen

[ ]  Zertifizierung nach ISO 27001

[ ]  Zertifizierung nach ISO 27701

[ ]  Zertifizierung nach IT-Grundschutz

[ ]  Verhaltensregeln nach Art. 40 DS-GVO:

[x]  Klicken Sie hier, um Text einzugeben.

1. Klauseln der Kommission vom 5. Februar 2010: <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087> [↑](#footnote-ref-1)
2. Klauseln der Kommission vom 27. Dezember 2004: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32004D0915 [↑](#footnote-ref-2)
3. Martini M. Art. 35 Rn. 15 in Plath (Hrsg.) BDSG/DS-GVO: Kommentar zum BDSG und zur DS-GVO sowie den Datenschutzbestimmungen des TMG und TKG. ottoschmidt Verlag 2016. ISBN 978-3-504-56074-4 [↑](#footnote-ref-3)
4. Vergleiche hierzu aber auch die Ausführungen im Kurzpapier 18 der DSK (Online, zitiert am 2019-08-23; Verfügbar unter <https://www.datenschutzkonferenz-online.de/kurzpapiere.html>), welches auf Seite 5 in der Risikomatrix davon ausgeht, dass bei jeder Verarbeitung mindestens ein geringes Risiko für die Rechte und Freiheiten betroffener Personen existiert.

Demgegenüber ist jedoch Erwägungsgrund 80 DS-GVO (<https://ds-gvo.gesundheitsdatenschutz.org/html/ds-gvo_2016_erwgr_080.php>) zu entnehmen, dass es Verarbeitungen gibt, welche wahrscheinlich kein Risiko beinhalten. [↑](#footnote-ref-4)
5. Bzgl. Lebensrisiko siehe auch: BGH Urt. V. 1993-05-04, AZ VI ZR 283/92. Online, zitiert am 2019-08-23; Verfügbar unter [https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=04.05.1993 &Aktenzeichen=VI%20ZR%20283/92](https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=04.05.1993&Aktenzeichen=VI%20ZR%20283/92) [↑](#footnote-ref-5)
6. BSI: Technische Richtlinie 02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Online, zitiert am 2017-09-03; Verfügbar unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index\_htm.html [↑](#footnote-ref-6)