SCHEJA & PARTNERS

PrivacyPilot

Methodische Anforderungen an eine toolgestützte Umsetzung des Standard-Datenschutzmodells (SDM)

09.09.2024

1. SDM setzt Verzeichnis von Verarbeitungstätigkeiten voraus

Kap. D4.1 SDM 3.1, S. 57

*Konkret muss der Verantwortliche gemäß **Art. 30 DS-GVO ein Verzeichnis** führen, in dem die personenbezogenen Verarbeitungstätigkeiten der Organisationen aufgelistet sind.*

Art. 30 DSGVO

Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:
[…]
*b) die **Zwecke** der Verarbeitung;*
*c) eine Beschreibung der **Kategorien betroffener Personen** und der **Kategorien personenbezogener Daten**;*

Kap. D2 SDM 3.1, S. 36

*Diese allgemeine Beschreibung einer Verarbeitung stellt noch **keine ausreichende Dokumentation** von Verarbeitungstätigkeiten dar […].*

Kap. D2.2 SDM 3.1, S. 39

*Die **Mittel**, die für eine Verarbeitung genutzt werden, sind ein **unverzichtbarer Bestandteil** der Verarbeitung.*

zu 1. Toolgestützte methodische Umsetzung

Ein SDM-konformes VVT muss neben den Artikel 30-Anforderungen die eingesetzten Betriebsmittel einbeziehen

System / Betriebsmittel
Krankenhaus-informationssystem (KIS)

Betroffene
Patient

Datenkategorie
Gesundheitsdaten

Zweck
Durchführung des Behandlungsvertrags

Zu beachten ist weiterhin, dass einige Betriebsmittel neben den personenbezogenen Daten der Verarbeitungstätigkeit, die das Betriebsmittel einsetzt, auch zusätzlich „eigene“ personenbezogene Daten verarbeiten (spezifische Betriebsmitteldaten, z. B. Benutzerverwaltungsdaten und E-Mail-Adressen bei einem Videokonferenzsystem) (Kap. D2.2 SDM 3.1, S. 40)

System / Betriebsmittel
Krankenhaus-informationssystem (KIS)

Betroffene
Beschäftigte

Datenkategorie
Authentifizierungs-informationen

Zweck
Sicherer Betrieb von IT-Systemen

2. SDM setzt materielle Rechtskonformität voraus

Kap. D2.4 SDM 3.1, S. 41

*Ob eine Verarbeitung einem **legitim gesetzten Zweck** folgt und ob der Zweck der Verarbeitung hinreichend bestimmt ist, muss vor der Anwendung des SDM geklärt sein.*

Kap. D3.1 SDM 3.1, S. 51

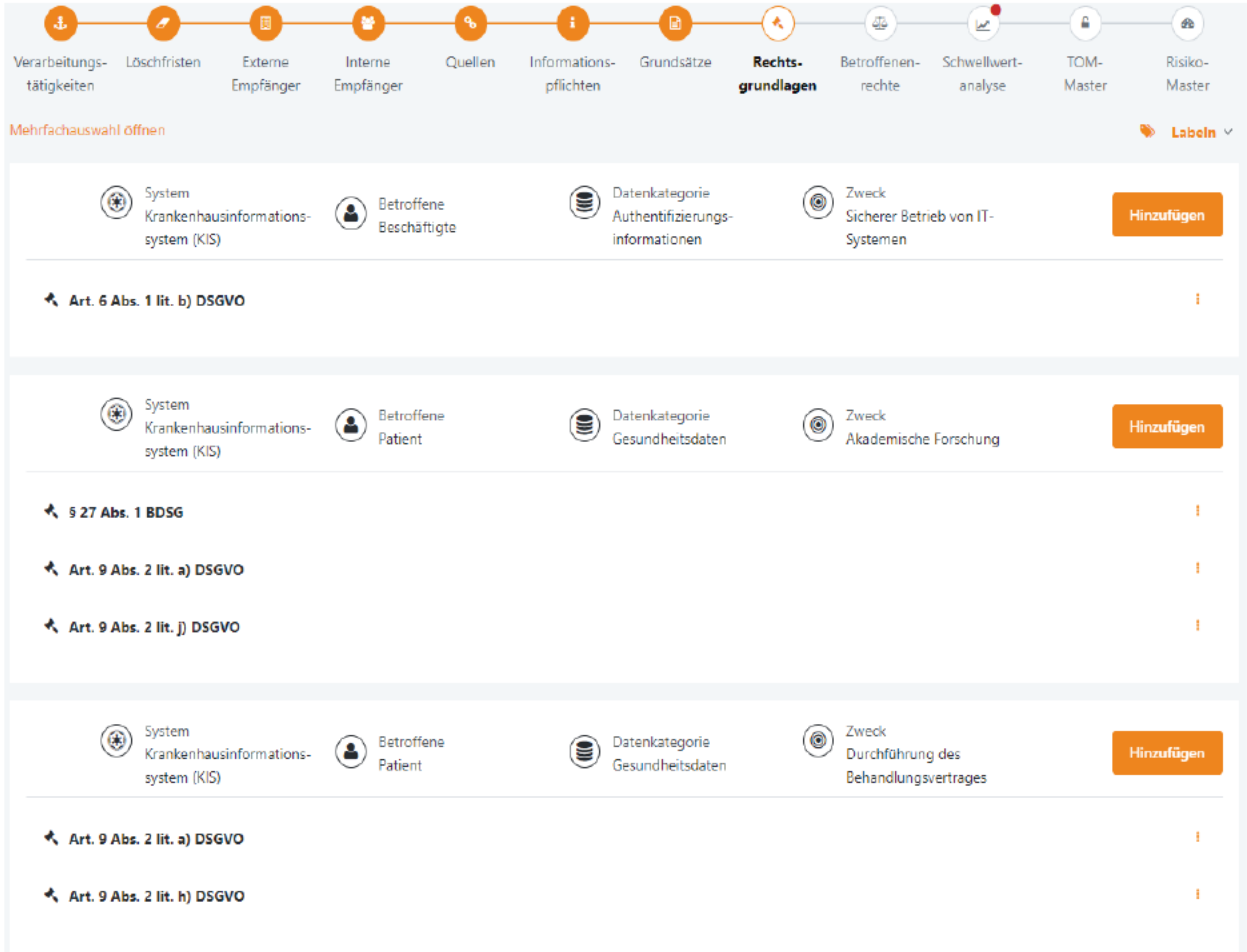
*Die Prüfung der **Verhältnismäßigkeit des Grundrechtseingriffs** einer Verarbeitung ist nicht vom SDM umfasst. Diese rechtliche Prüfung sowie die Prüfung der **Rechtsgrundlage nach Artikel 6 und ggf. 9 DS-GVO** müssen vor der Anwendung des SDM erfolgen.*

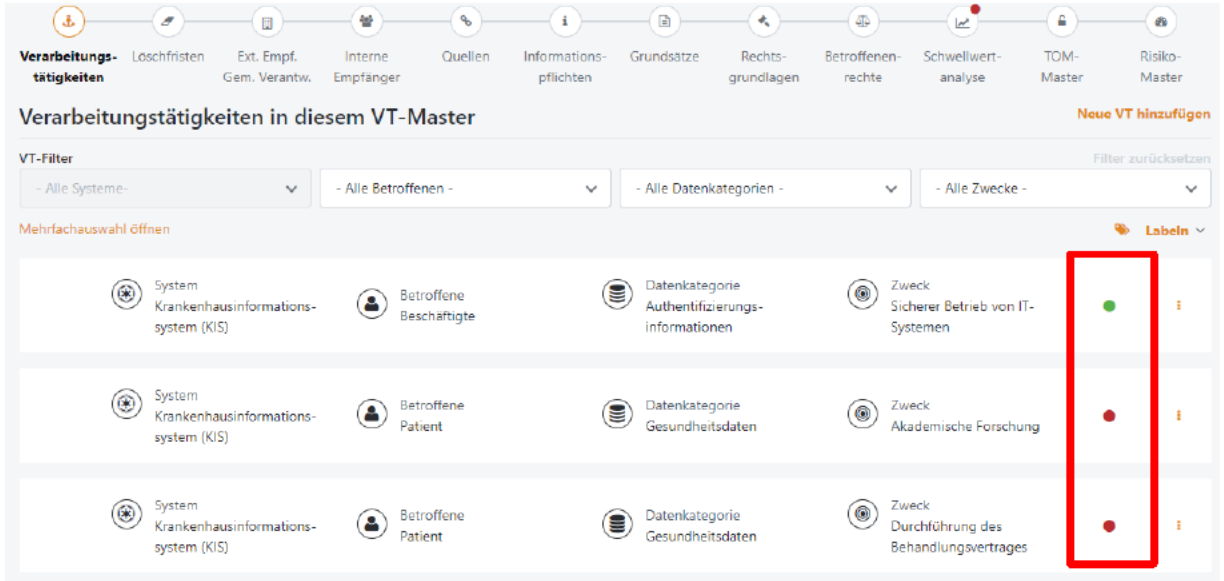
Kap. D3.2 SDM 3.1, S. 51

*Zur Bestimmung der Höhe des Risikos muss der Verantwortliche daher zunächst eine **„Schwellwert-Analyse“** durchführen. Diese Analyse muss für jede Verarbeitungstätigkeit, bestehend aus einem oder mehreren Verarbeitungsvorgängen, durchgeführt werden […] (Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO).*

zu 2. Toolgestützte methodische Umsetzung

Kernanforderungen der materiellrechtlichen Zulässigkeit nach DSGVO





3. SDM verlangt umfassende Risikobetrachtung

Kap. D2.6 SDM 3.1, S. 48

*Der **SDM-Würfel führt somit ein Gesamtbild zur Analyse der Risiken einer Verarbeitungstätigkeit** vor Augen. Dieses Gesamtbild ist insbesondere für komplexe Verarbeitungen nützlich, um systematisch die Vollständigkeit der Analyse, die Handlungsbedarfe und den Nachweis der Umsetzung der datenschutzrechtlichen Anforderungen und der Bearbeitung der Risiken sicherzustellen.*

Kap. D3.3 SDM 3.1, S. 54

Der **Schutzbedarf für betroffene Personen ergibt sich aus dem Risiko** der Verarbeitungstätigkeit, **bevor technische und organisatorische Maßnahmen** bestimmt und umgesetzt wurden. Insofern gilt der folgende Zusammenhang zwischen Risiko(höhe), im Sinne eines Ausgangsrisikos, und Schutzbedarf(sstufe):

- **kein oder geringes Risiko** der Verarbeitung ➔ normaler Schutzbedarf für von der Verarbeitung betroffene Personen
- **normales Risiko** der Verarbeitung ➔ normaler Schutzbedarf für von der Verarbeitung betroffene Personen
- **hohes Risiko** der Verarbeitung ➔ hoher Schutzbedarf für von der Verarbeitung betroffene Personen

zu 3. Toolgestützte methodische Umsetzung

Abbildung des SDM-Würfels als zweidimensionale Matrix

Risikobewertung vor Umsetzung technischer und organisatorischer Maßnahmen

Risiko ergibt den Schutzbedarf. Dieser indiziert den SOLL-Zustand

4. SDM erfordert systematische Bestimmung von TOM

Kap. D4.1 SDM 3.1, S. 57

(Es) ***müssen geeignete technische und organisatorische Maßnahmen bestimmt und dauerhaft umgesetzt werden****, um ein dem Risiko angemessenes Schutzniveau bei jeder Verarbeitung personenbezogener Daten zu gewährleisten.*

Kap. D4.1 SDM 3.1, S. 57

Damit der Verantwortliche den detaillierten Anforderungen in Bezug auf die operative Umsetzung der Betroffenenrechte und seinen Rechenschafts- und Nachweispflichten (vgl. Abschnitt B1.8) nachkommen kann, ist eine ***systematische Vorgehensweise*** *bei der Prüfung und Beurteilung erforderlich, die sich [auf] die dazu gehörigen* ***technischen und organisatorischen Maßnahmen*** *bezieht.*

Kap. D3.4 SDM 3.1, S. 56

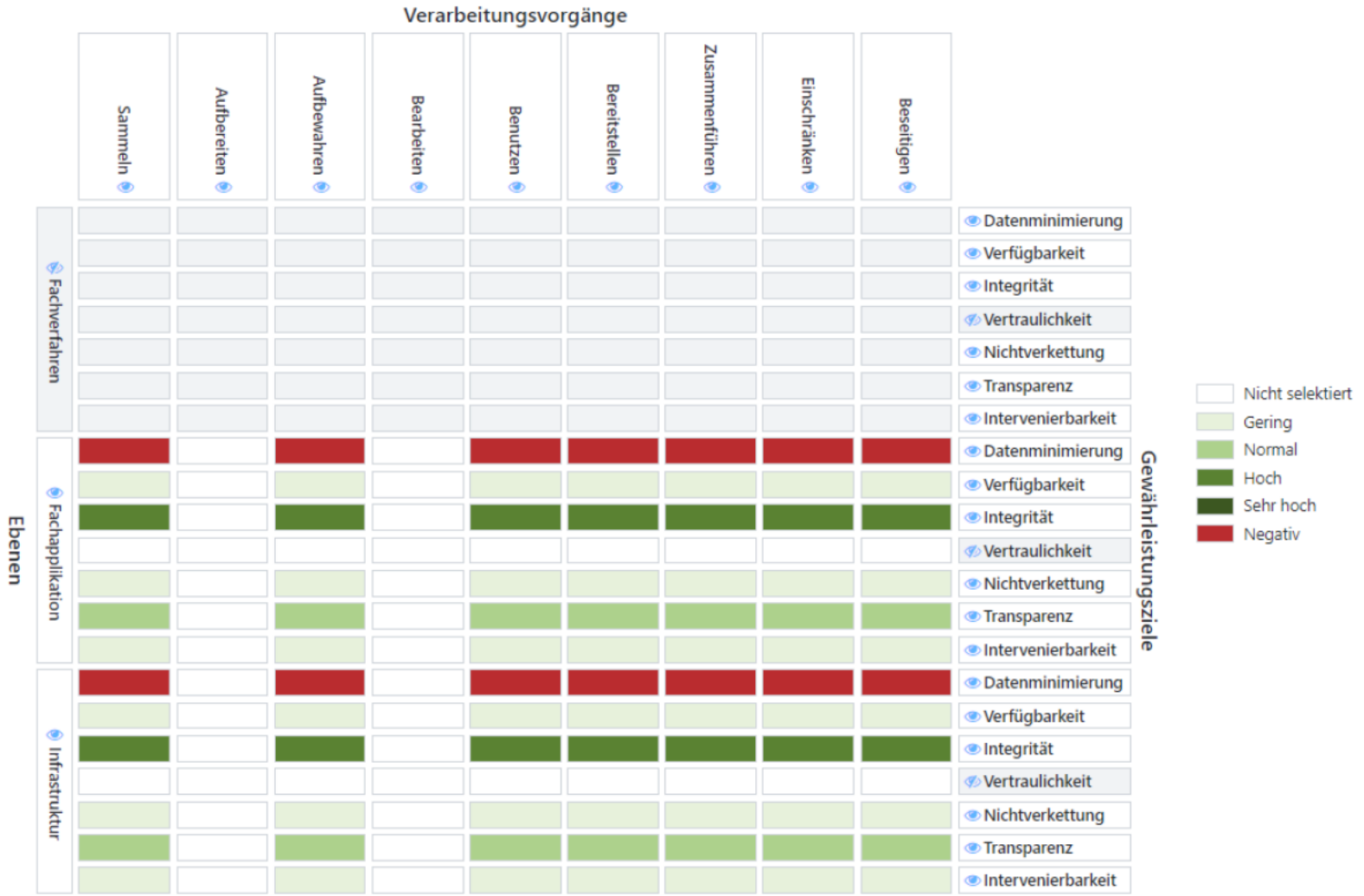
Zu beachten ist, dass ***neue Risiken*** *durch ergriffene technische und organisatorische Maßnahmen entstehen können*

zu 4. Toolgestützte methodische Umsetzung

Systematische Klassifizierung von TOM nach dem SDM-Würfel (Mitigationspotential)

Implementierung der TOM setzt Mitigationspotential um und ändert IST-Zustand

Einheitliche Methode hinsichtlich IST- und SOLL-Zustand gewährleistet Vergleichbarkeit zwischen Risiko und Mitigationspotential



5. Mit dem SDM zur Datenschutz-Folgenabschätzung

Kap. A1 SDM 3.1, S. 8

*Das SDM bietet eine **Systematik, um eine DSFA in strukturierter Form zu erarbeiten**.*

Einleitung SDM 3.1, S. 6

*TOM können herangezogen werden, „um bei jeder einzelnen Verarbeitung zu prüfen, ob das rechtlich geforderte **„Soll“** von Maßnahmen mit dem vor Ort vorhandenen **„Ist“** von Maßnahmen übereinstimmt.*

Kap. D2.6 SDM 3.1, S. 45

*Erst durch die **Einbeziehung aller Komponenten auf den verschiedenen Ebenen** ist eine angemessene Untersuchung und Beurteilung eines Verarbeitungsvorgangs möglich.*

zu 5. Toolgestützte methodische Umsetzung

Benutzerdefinierte Selektion von Risiken zur Anzeige relevanter TOM unter Angabe ihres Mitigationspotentials

Systematische Ermittlung des verbleibenden Restrisikos unter Nutzung der SDM-Methodik

Vorschlag geeigneter weiterer TOM mit entsprechendem Mitigationspotential

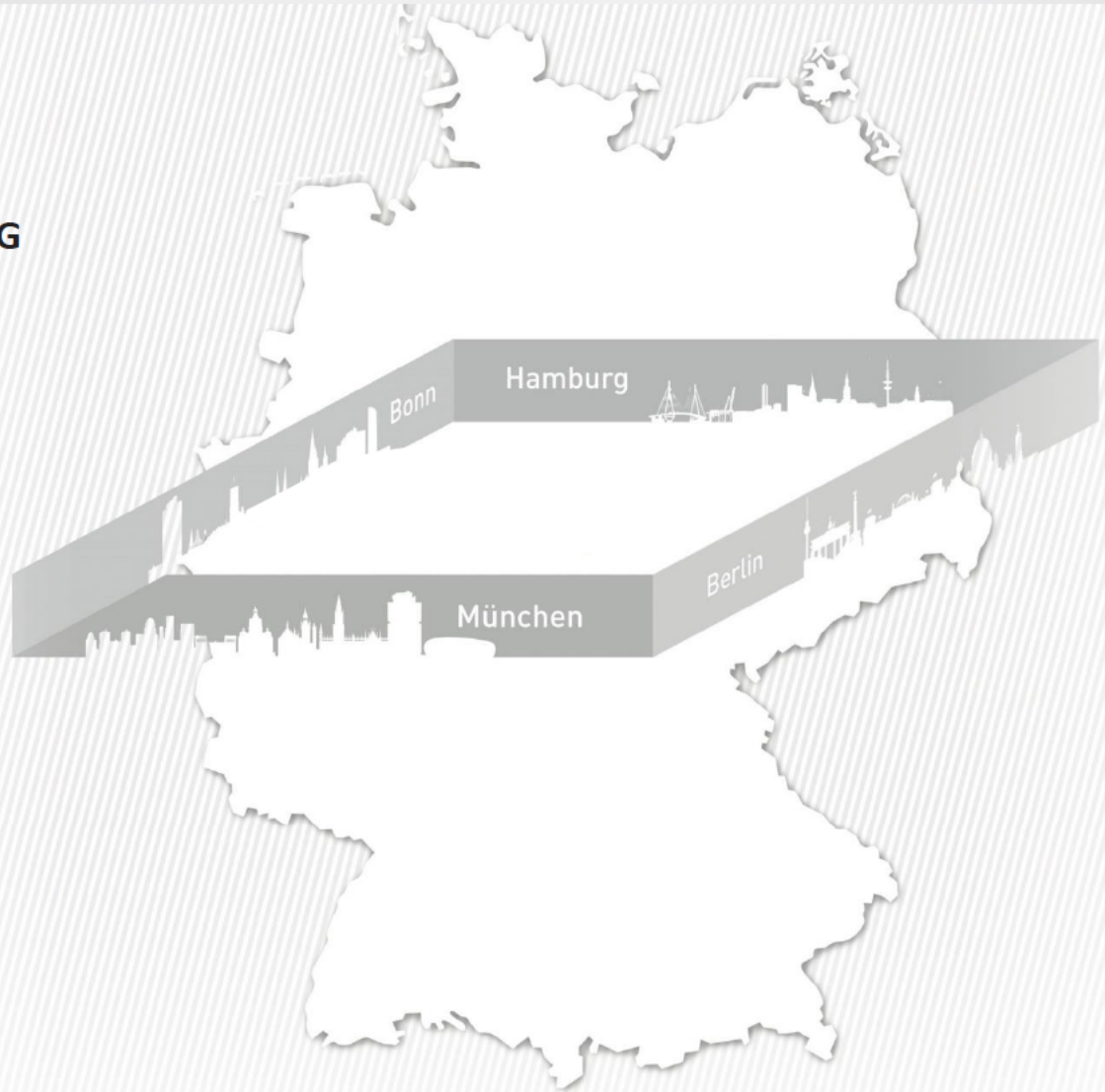
Kontakt

Scheja & Partners GmbH & Co. KG

+49 228 227 226-0
info@scheja-partners.de
www.scheja-partners.de

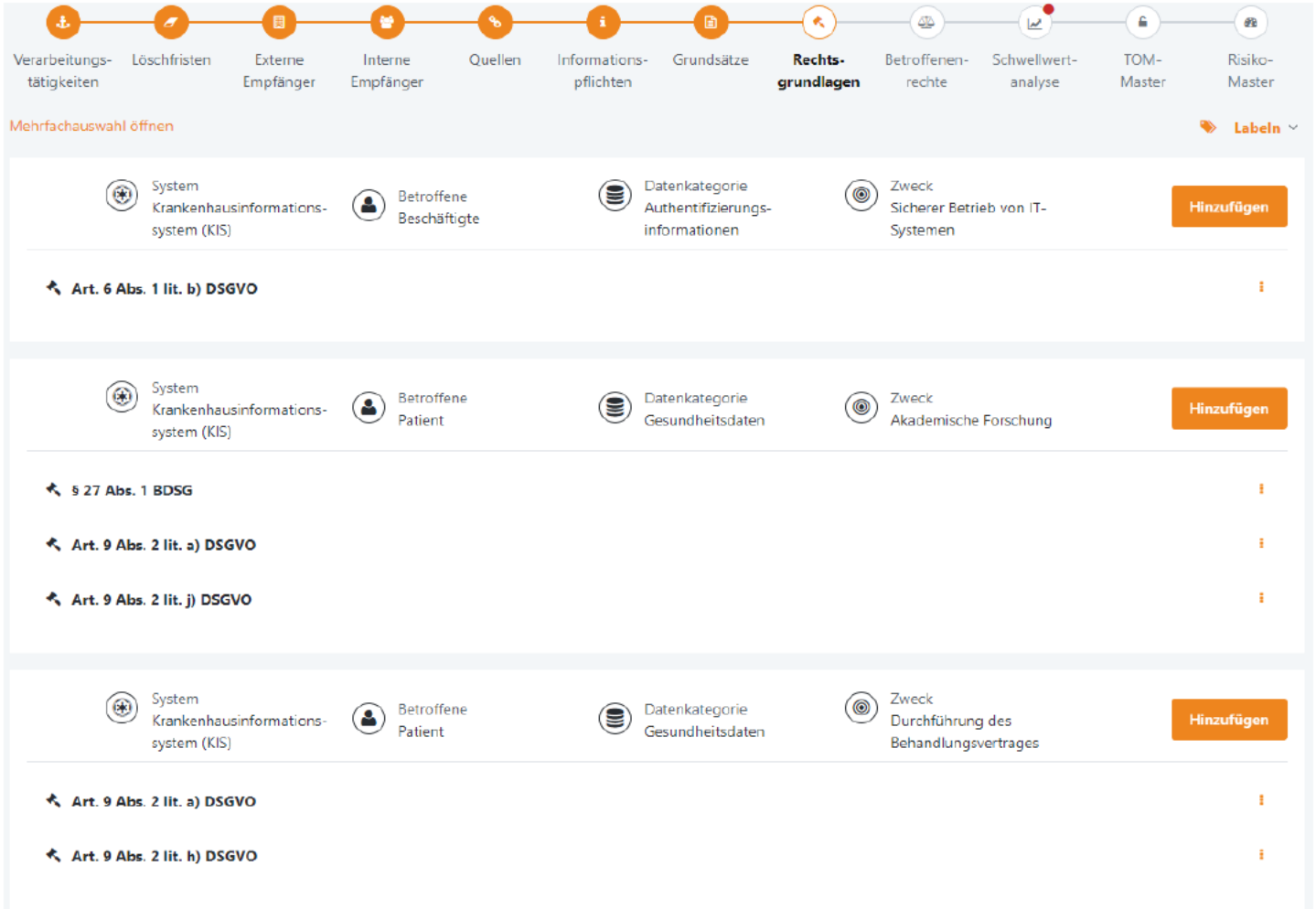
PrivacyPilot GmbH

+49 228 504 46 270
info@privacy-pilot.com
www.privacy-pilot.com



zu 2. Toolgestützte methodische Umsetzung

Kernanforderungen der materiellrechtlichen Zulässigkeit nach DSGVO



zu 5. Toolgestützte methodische Umsetzung

Benutzerdefinierte Selektion von Risiken zur Anzeige relevanter TOM unter Angabe ihres Mitigationspotentials

Systematische Ermittlung des verbleibenden Restrisikos unter Nutzung der SDM-Methodik

Vorschlag geeigneter weiterer TOM mit entsprechendem Mitigationspotential

Technische und organisatorische Maßnahmen

Bezeichnung	TOM-Master	Katalog	Baustein	Schutzklasse
Filter	- Alle -	- Alle -	- Alle -	- Alle -
Aufbewahrungssicherung (Safe, getrennter Brandabschnitt etc.)	Klinik-Informations-System (KIS)	Technische und Organisatorische (Schutz-)maßnahmen gemäß Art. 32 Abs. 1 DSGVO	Verfügbarkeitskontrolle	Hoch
Differenziertes Rollenkonzept (Arzt, Pflege, Verwaltung etc.)	Klinik-Informations-System (KIS)	Technische und Organisatorische (Schutz-)maßnahmen gemäß Art. 32 Abs. 1 DSGVO	Zwecktrennung	Hoch
Elektronische Zutrittskontrolle	Klinik-Informations-System (KIS)	Technische und Organisatorische (Schutz-)maßnahmen gemäß Art. 32 Abs. 1 DSGVO	Zutrittskontrolle	Hoch
Löschung nach Ablauf der Löschfrist	Klinik-Informations-System (KIS)	Technische und Organisatorische (Schutz-)maßnahmen gemäß Art. 32 Abs. 1 DSGVO	Zugriffskontrolle	Normal
Nutzerbezogene Kenn- und Passwörter	Klinik-Informations-System (KIS)	Technische und Organisatorische (Schutz-)maßnahmen gemäß Art. 32 Abs. 1 DSGVO	Zugangskontrolle	Gering
Protokollierung und Überprüfung der Zugriffe	Klinik-Informations-System (KIS)	Technische und Organisatorische (Schutz-)maßnahmen gemäß Art. 32 Abs. 1 DSGVO	Zugriffskontrolle	Normal
Rollenprinzip: Nicht mehr Rechte als nötig	Klinik-Informations-System (KIS)	Technische und Organisatorische (Schutz-)maßnahmen gemäß Art. 32 Abs. 1 DSGVO	Zugriffskontrolle	Hoch