gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Verzeichnis von Verarbeitungstätigkeiten

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Agenda

- Vorschrift der DSGVO (Artikel 30)
- Welche Verarbeitungstätigkeiten betrifft das?
- Möglichkeiten zur praxisnahen Umsetzung

- Datenschutzfolgenabschätzung
- Risikomanagement
- Konsultation der Aufsichtsbehörde

Verzeichnis von Verarbeitungstätigkeiten

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Das Verzeichnis von Verarbeitungstätigkeiten muss aufgestellt werden, wenn das Unternehmen mindestens 250 Mitarbeiter hat.

ODER

- Wenn Daten mit Risiken für die Rechte und Freiheiten der betroffenen Personen verarbeitet werden,
  - **insbesondere Verarbeitung besonderer Datenkategorien**
  - personenbezogene Daten über strafrechtliche Verurteilungen

ODER

- die Datenverarbeitung erfolgt nicht nur gelegentlich

<u>Offen</u>: Es müssen nach Artikel 30 DSGVO alle Unternehmen die eingesetzten Verarbeitungen dokumentieren, nach EWG 13 sollen kleine und mittlere Unternehmen (bis 250 MA) entlastet werden !

(das Verzeichnis gilt übrigens auch manuelle Verarbeitungen!)

→ Artikel 30 DSGVO

Kurzpapier Nr. 1 der DSK:
https://www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf

Sinn des Verzeichnisses

- Übersicht für den Datenschutzbeauftragten und auch Teil des DSMS, das der DSB zu überwachen hat

- Arbeitsgrundlage für die Aufsichtsbehörde, der das aktuelle Verzeichnis auf Anfrage zur Verfügung zu stellen ist (EWG 82)

- Im Falle der nicht ordnungsgemäßen Führung:
  - Geldbußen von bis zu **10 000 000 EUR** oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist

Verzeichnis von Verarbeitungstätigkeiten

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Personaldatenverarbeitung
  - Adressdaten von Mitarbeitern, Rentnern (ehemaligen Mitarbeitern)
  - Bewerbungsdaten, Personalplanung,
  - Lohn- und Gehaltsdaten,
  - Zeiterfassung,
  - Reisekosten,
  - Excel - Mitarbeitergespräche
  - **auch manuelle Personalakten**
- Patientendatenverarbeitung
  - QS Monitor – Qualitätsmanagement
  - ODS easy – Tumordokumentation
  - ORBIS – alle selbständigen Module!
  - Hi-med Siemens – Telefonabrechung Patienten
  - SAP – Fibu
  - MobiDik – Patientenbezogene Verbrauchserfasssung
  - **auch manuelle Akten von Patienten / Probanten / Studienteilnehmern**

Es ist zu dokumentieren für Verantwortliche

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Namen und Kontaktdaten des Verantwortlichen
- Namen und Kontaktdaten des Datenschutzbeauftragten
- die Zwecke der Verarbeitung
- eine Beschreibung der Kategorien betroffener Personen
- eine Beschreibung der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, einschließlich Empfänger in Drittländern
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland, sowie die Dokumentierung geeigneter Garantien für den Datenschutz
- die Fristen für die Löschung der verschiedenen Datenkategorien;
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Fazit: sehr ähnlich dem bisherigen BDSG !

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Für Verantwortliche

§ 4e BDSG	Art. 30 DS-GVO
– Name oder Firma der verantwortlichen Stelle – Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter – Anschrift der verantwortlichen Stelle	Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen
Die mit der Leitung der Datenverarbeitung beauftragten Personen,	Namen und die Kontaktdaten eines etwaigen Datenschutzbeauftragten
Zweckbestimmungen der Datenerhebung, -verarbeitung oder –nutzung	Zwecke der Verarbeitung
Beschreibung der betroffenen Personengruppen	Beschreibung der Kategorien betroffener Personen
Beschreibung der Daten oder Datenkategorien	Beschreibung der Kategorien personenbezogener Daten
Empfänger oder Kategorien von Empfängern	Kategorien von Empfängern […], einschließlich Empfänger in Drittländern oder internationalen Organisationen
Regelfristen für die Löschung der Daten	die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
Geplante Datenübermittlung in Drittstaaten	Kategorien von Empfängern […], einschließlich Empfänger in Drittländern oder internationalen Organisationen
Allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind	eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32

Es ist auch zu dokumentieren

Die Dokumentation der datenschutzkonformen Verarbeitung verlangt noch weitere Angaben, die sich nicht aus Artikel 30 DSGVO ergeben:

- Rechtsgrundlage für die Verarbeitung (Art. 6 DSGVO)
- Verweis auf Vertragsgestaltung mit Dritten (Art. 28 DSGVO)
- Datenübermittlung in Drittländer
- Riskoabschätzung / Risikobewertung
- Hinweis auf Datenschutz – Folgeabschätzung (Art. 35 DSGVO)

„Das genannte Verzeichnis ist schriftlich zu führen,
was auch in einem elektronischen Format erfolgen kann.“

Neu: Es ist zu dokumentieren für Auftragsverarbeiter

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Namen und Kontaktdaten des oder der Auftragsverarbeiter
- Namen und Kontaktdaten jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist,
- Name und Kontaktdaten des Datenschutzbeauftragten
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland sowie die Dokumentierung geeigneter Garantien;
- allgemeine Beschreibung der technischen und organisatorischen Datensicherheits - Maßnahmen.

Fazit: Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter ist ganz neu !

Für Auftragsverarbeiter

§ 4e BDSG	Art. 30 DS-GVO
	den Namen und die Kontaktdaten des Auftragsverarbeiters
	den Namen und die Kontaktdaten eines etwaigen Datenschutzbeauftragten des Auftragsverarbeiters
	Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden
	gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien
	eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32

Übersicht über Verfahren

	Erfassung der eingesetzten Verfahren				
Übersicht für den Bereich XYZ					
Name des Programmes in dem personenbezogene Daten gespeichert oder verarbeitet werden	Ansprechpartner / Verantwortlicher - wen kann man ggf. fragen?	Zweck des Programmes, d.h. wozu wird es verwendet?	Wer greift noch auf die Daten zu bzw. verarbeitet diese (Kliniken, Abtei-lungen innerhalb des KH)	hat ein externer Dienst-leister (außerhalb des KH) Datenzugriff	gibt es mit dem Dienst- leister eine aktuelle Datenschutzregelung?
ORBIS Patientenaufnahme	Frau Adam	Patientenaufnahme	Kliniken, Funktions-Abteilungen, Controlling Finanzbuchhaltung	Fa. Agfa	Ja, im Vertragsmanagement dokumentiert
SAP Fibu	Herr Bertram	Finanzbuchhaltung - Wahlleistungsentgelte	Controlling	Fa. BTC	Ja, im Vertragsmanagement dokumentiert
Tumordokumentation	Frau Celias	Tumordokumentation	Onkologie	Nein	

Erfassung mit Excel?

Übersicht über Verarbeitungen mit personenbezogenen / personenbeziehbaren Daten												
Verantwortliches Unternehmen / Abteilung					DS-Koordinator:				Stand:			
Unter-nehmen / Abteilung	Name der Verarbeitung / interner Geschäftsprozess	Zweck der Verarbeitung	Kategorien der Daten	Rechtsgrundlage der Verarbeitung (rechtliche Vorschrift(1), Vertrag(2), berechtigtes Interesse(3), Einwilligung(4))	Sensibilität - Risiko (gering (A); mittel (B), hoch (C))	Datenschutz-Folgenabschätzung (DSFA)	Löschfristen	Drittland-übermittlung außerhalb EU	externe Dienst- leister	Vertrag zur Auftrags-verarbeitung?	TOM´s	Prüf-vermerk DSB
Beispiele:												
Kranken-haus Aufnahme	ORBIS - Aufnahme	Aufnahme aller Patienten	Name, Kontaktdaten, Versichertendaten, Überweisung	2 (Behandlungsvertrag)	C (Besondere Schutz-maßnahmen sind erforderlich)	erforderlich	30 Jahre nach Behandlung	nein	Agfa	Ja, AV-Vertrag mit Agfa	im AV-Vertrag mit Agfa enthalten	
Pflege-schule	Schülerverzeichnis	Nachweis der Ausbildung	Name, Kontaktdaten, Ausbildungsinhalte und -ergebnisse	2 (Ausbildungsvertrag)	B	nicht erforderlich	keine Löschung, weil Ausbildungsnachweis	nein	BCT	Ja, AV-Vertrag mit BCT	im AV-Vertrag mit BCT enthalten	

Verzeichnis von Verarbeitungstätigkeiten

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Stand der Erfassung: .....

Namen des / der Verantwortlichen .....

Anschrift des Verantwortlichen .....

.....

Geschäftsführer ..... **Tel./E-Mail:** .....

Datenschutzbeauftragter ..... **Tel./E-Mail:** .....

Verantwortlich für diese Verarbeitung: Abteilung / Name des Verantwortlichen ..... **Tel./E-Mail:** .....

Inhalt der Meldung	**Beschreibung der automatisierten Verarbeitung**
Name des Verfahrens / Anwendung / Programms / Prozesses	.....
Zweckbestimmung der Datenerhebung, -verarbeitung und -nutzung	.....(wozu nutzt man das Programm).....
Beschreibung der betroffenen Personengruppen	☐ Mitarbeiter ☐ Patienten ☐ Lieferanten ☐ Sonstige: .....(die Gruppe der Betroffenen Ankreuzen oder nennen)
Beschreibung der diesbezüglichen Daten oder Datenkategorien	.....(welche Art von Daten werden verarbeitet).....
Regelfristen für die Löschung der Daten	.....(wann wird ein konkretes Datum wieder gelöscht, z.B. 10 Jahre nach Beendigung des Vertrages)
Interne Empfänger von Daten	Abteilung: ..... Art der Daten: ..... Zweck des Transfers: .....
Externe Empfänger von Daten	Stelle: ..... Art der Daten: ..... Zweck der Übermittlung: .....
Datenübermittlung ins Drittland	Welche Staaten: ..... Welche vertraglichen Regelungen bestehen: .....

Zulässigkeit der Verarbeitung	☐ Vertrag, Vorvertragsverhältnis ☐ Einwilligung des Betroffenen ☐ Vorrangige Rechtsvorschrift: ..... ☐ Interessenabwägung ☐ Sonstige: .....
Auftragsverarbeitung liegt vor: Vertragsbestandteile sind vorhanden: Geprüft am:	☐ JA (Wenn ja, dann muss der schriftliche Vertrag die hier genannten Punkte beinhalten) ☐ Gegenstand und die Dauer des Auftrags, ☐ Umfang, Art und der Zweck der Verarbeitung ☐ Art der Daten und der Kreis der Betroffenen, ☐ technisch-organisatorischen Maßnahmen ☐ Berichtigung, Löschung, Sperrung von Daten, ☐ Pflichten des Auftragnehmers (Kontrollen) ☐ Genehmigung von Unterauftragsverhältnissen, ☐ Kontrollrechte des Auftraggebers ☐ Mitteilungen über Datenschutz-Verstöße ☐ Weisungsbefugnisse des Auftraggebers ☐ Rückgabe / Löschung von Datenträgern / Daten .....
Information der Betroffenen:	Erfolgte durch: ☐ Information bei Vertragsabschluss ☐ Separates Anschreiben ☐ Internet-Datenschutzerklärung ☐ Sonstiges: .....
Risikobewertung	☐ Persönlichkeitsschaden ist eher unwahrscheinlich ☐ Persönlichkeitsschaden ist entfernt denkbar ☐ Persönlichkeitsschaden kann eintreten ☐ Anmerkung: .....
Datenschutz - Folgeabschätzung	☐ Nicht erforderlich, weil kein hohes Risiko ☐ Erforderlich und durchgeführt am: mit dem Ergebnis: Meldung an die Aufsichtsbehörde ☐ Nicht erforderlich ☐ Erforderlich und durchgeführt am: mit dem Ergebnis: ☐ Wiedervorlage ☐ Nicht erforderlich ☐ Erforderlich am:
Getroffene Datensicherungsmaßnahmen (hinsichtlich: Vertraulichkeit, Verfügbarkeit und Integrität Belastbarkeit, Wiederanlauf, Prüfbarkeit)	☐ Datensicherheitskonzept ☐ siehe Datensicherheitsbeschreibung (TOM´s) ☐ sonstiges:

....

Verarbeitungsverantwortlicher: Datum: Unterschrift:

Technischen und organisatorischen Maßnahmen gemäß Anlage zu § 9 BDSG

Organisation des Datenschutzes

Technische Maßnahmen

1 Zutrittskontrolle

2. Zugangskontrolle

3 Zugriffskontrolle

4 Weitergabekontrolle

5 Eingabekontrolle

6 Auftragskontrolle

7 Verfügbarkeitskontrolle

8 Trennungsgebot

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Technische und organisatorische Maßnahmen
gemäß Artikel 32 Abs. 1 DSGVO

1. Gewährleistung der Vertraulichkeit*

2. Gewährleistung der Integrität*

3. Gewährleistung der Verfügbarkeit*

4. Gewährleistung der Belastbarkeit der Systeme*

5. Wiederherstellung der Verfügbarkeit*

6. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen*

Es liegen schriftlich vor
- ☐ interne Verhaltensregeln
- ☐ Risikoanalyse
- ☐ allgemeine Datensicherheitsbeschreibung
- ☐ umfassendes Datensicherheitskonzept
- ☐ Wiederanlaufkonzept
- ☐ Zertifikat:
  Zertifizierungsstelle
- ☐ Sonstiges

* ergänzende Angaben auf einem Extrablatt

…….. Datum

…… Unterschrift

Datenschutz – Folgenabschätzung

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Notwendig im Vorfeld von Datenverarbeitungen, die voraussichtlich ein hohes Risiko für persönliche Rechte und Freiheiten der Betroffenen aufweisen
  - → Risikoanalyse notwendig!
  - → formale Bearbeitung der DSFA

  → Konsultationspflicht der Aufsichtsbehörde, fall das Ergebnis ein hohes Risiko nahelegt **und** der Verantwortliche **trifft keine** Maßnahmen zur Eindämmung des Risikos:
    - Aufsichtsbehörde kann binnen 8 Wochen eine Empfehlung zur Risikominimierung abgeben

      oder
    - Aufsichtsbehörde kann eine Untersagung der Datenverarbeitung aussprechen

→ Artikel 35 DSGVO

Kurzpapier Nr. 5 der DSK:
https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf

Wann ist eine DSFA vorzunehmen?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Nach Art. 35 Abs. 1 DSGVO ist eine DSFA grundsätzlich immer dann durchzuführen wenn:

- „(…) eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge (hat)“.
- Darüber hinaus Regelbeispiele für Durchführungspflichten (Art. 35 Abs. 3 DSGVO):
  - systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen;
  - umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Abs. 1 oder von Daten über strafrechtl. Verurteilungen / Straftaten
  - systematische weiträumige Überwachung öffentlich zugänglicher Bereiche

Entspricht weitgehend der aus dem BDSG bekannten Vorabkontrolle (§ 4d Abs. 5)

UND: Wenn eine DSFA notwendig ist, dann ist auch ein DSB zu bestellen!

- Die Aufsichtsbehörden müssen gemäß Art. 35 Abs. 4 DSGVO im Rahmen ihres jeweiligen Zuständigkeitsbereichs eine Liste der Verarbeitungsvorgänge erstellen u. veröffentlichen, für die eine DSFA nach Abs. 1 durchzuführen ist.
- Die Aufsichtsbehörden können gemäß Art. 35 Abs. 5 DSGVO eine Liste der Verarbeitungsvorgänge erstellen und veröffentlichen, für die keine DSFA durchgeführt werden muss.

  → DSK: es wird keine „Negativliste“ geben

- **Fazit**:
  - Solange die Aufsichtsbehörden keine Listen vorgelegt haben, können sie keine Vorabkontrolle verlangen!
  - Tipp: Dennoch bei sensitiven Daten, Videoüberwachung, CRM-Systemen etc. gleich eine formale Vorabkontrolle durchführen!

Risikomanagement

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

https://de.wikipedia.org/wiki/Risikomanagement

- Risikomanagement ist nach der Norm ISO 31000: 2009 eine Führungs-aufgabe, im Rahmen derer die Risiken einer Organisation identifiziert, analysiert und bewertet werden. Hierzu sind übergeordnete Ziele, Strategien und Politik der Organisation für das Risikomanagement festzulegen.
- Im Einzelnen betrifft dies die Festlegung von Kriterien, nach denen die Risiken eingestuft und bewertet werden, die Methoden der Risikoermittlung, die Verantwortlichkeiten bei Risikoentscheidungen, die Bereitstellung von Ressourcen zur Risikoabwehr, die interne und externe Kommunikation über die identifizierten Risiken (Berichterstattung) sowie die Qualifikation des Personals für das Risikomanagement.
- Risikomanagement wird als ein fortlaufender Prozess verstanden, in dem Planung, Umsetzung, Überwachung und Verbesserung kontinuierlich statt-finden (PDCA-Zyklus: „Plan-Do-Check-Act“). Risikomanagement soll über die gesamte Lebensdauer einer Organisation zur Anwendung kommen und eine Kultur der Risikolenkung in der Organisation entstehen lassen.

Der Risikomanagement-Prozess umfasst im Einzelnen:

- Identifikation der Risiken, Beschreibung ihrer Art, der Ursachen und Auswirkungen
- Analyse der identifizierten Risiken hinsichtlich ihrer Eintrittswahrscheinlichkeiten und möglichen Auswirkungen
- Risikobewertung durch Vergleich mit zuvor festzulegenden Kriterien der Risiko-Akzeptanz (z. B. aus Standards und Normen)
- Risikobewältigung/Risikobeherrschung durch Maßnahmen, die Gefahren und/oder Eintrittswahrscheinlichkeiten reduzieren oder die Folgen beherrschbar machen
- Risikoüberwachung mit Hilfe von Parametern, die Aufschluss über die aktuellen Risiken geben (Risikoindikatoren)
- Risikoaufzeichnungen zur Dokumentation aller Vorgänge, die im Zusammenhang der Risikoanalyse und -beurteilung stattfinden

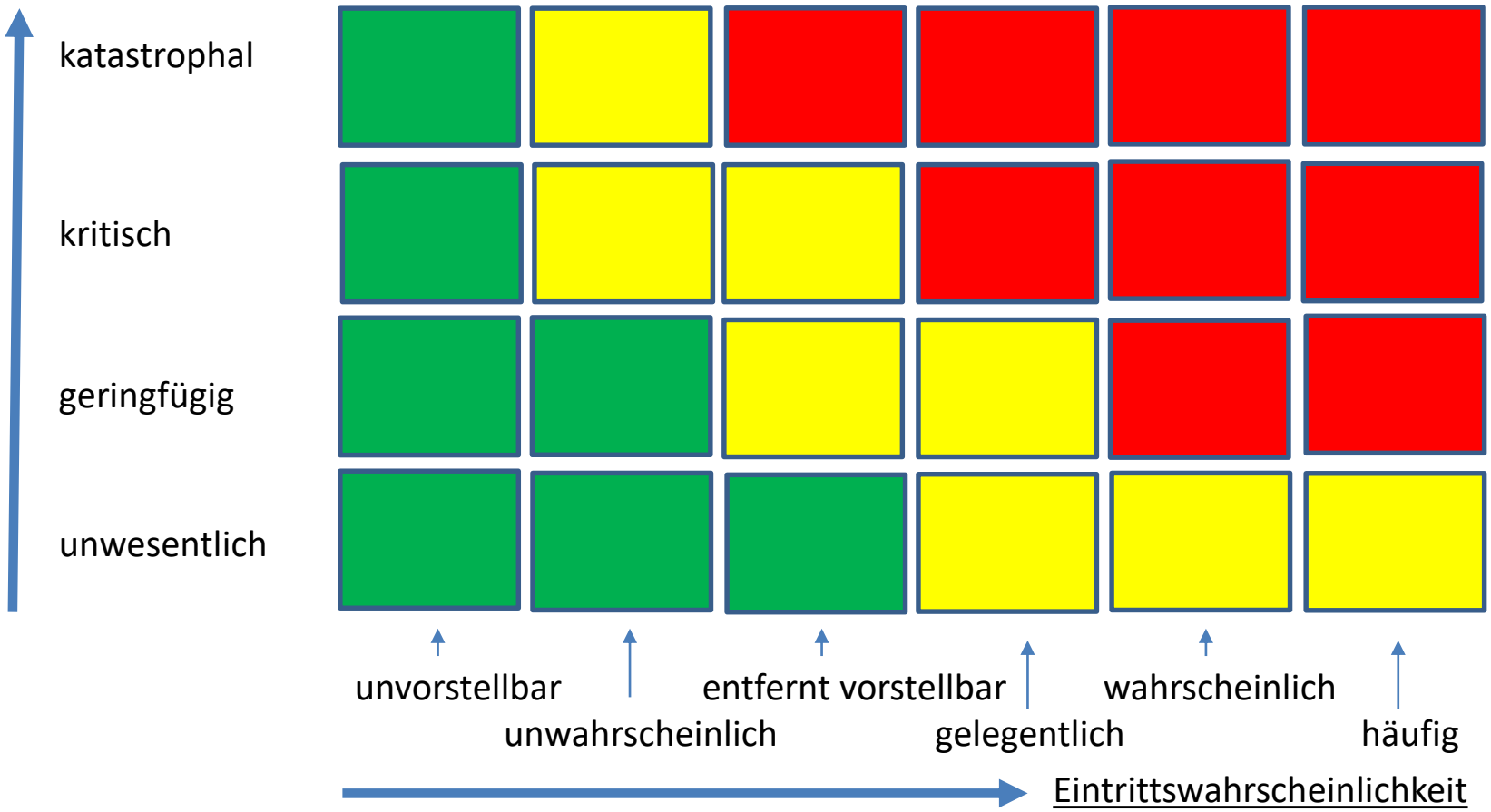
Risikograph

Akzeptabel

Risiko = Eintrittswahrscheinlichkeit * Schaden

Noch vertretbar

Inakzeptabel



Risikobewertung im Sinne des Datenschutzes

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Schaden:

- Katastrophal = Existenziell bedrohend für den Einzelnen
- Kritisch = Erhebliche Einschränkung der gesellschaftlichen oder persönlichen Stellung des Einzelnen
- Geringfügig = Geringe Einschränkung der gesellschaftlichen oder persönlichen Stellung des Einzelnen
- Unwesentlich = Keine Einschränkung der gesellschaftlichen oder persönlichen Stellung des Einzelnen

Risiko als Produkt von Schadenshäufigkeit und Schadenshöhe:

→ **Inakzeptable = Hohe Risiken**
sind durch geeignete Schutzmaßnahmen zu minimieren !

Inhalt der DSFA

Mindestanforderungen:

- systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen.
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck.
- Bewertung der Risiken der Rechte und Freiheiten der betroffenen Personen.
- Zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen werden soll.
- Bei der Durchführung einer Datenschutz-Folgenabschätzung ist zudem stets der Rat des Datenschutzbeauftragten (sofern ein solcher benannt wurde) einzuholen (Art. 35 Abs. 2 DSGVO)

→ Artikel 35 Abs. 7 DSGVO

Vorherige Konsultation der Aufsichtsbehörde

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

- Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichts-behörde, wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

- Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung gemäß Absatz 1 nicht im Einklang mit dieser Verordnung stünde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, unterbreitet sie dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu acht Wochen nach Erhalt des Ersuchens um Konsultation entsprechende schriftliche Empfehlungen und kann ihre in Artikel 58 genannten Befugnisse ausüben…..

→ Artikel 36 DSGVO

- Der Verantwortliche stellt der Aufsichtsbehörde bei einer Konsultation …. folgende Informationen zur Verfügung:
  - gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;
  - die Zwecke und die Mittel der beabsichtigten Verarbeitung;
  - die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen Maßnahmen und Garantien;
  - gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten
  - die Datenschutz-Folgenabschätzung gemäß Artikel 35 und
  - alle sonstigen von der Aufsichtsbehörde angeforderten Informationen.

Praktische Aspekte

- Folgenabschätzungen für alle relevanten Bestandsverfahren durchführen

Hinweis: wp 248 rev. 1 ARTICLE 29 DATA PROTECTION WORKING PARTY vom 04.10.2017: Hospital Information System braucht zwingend eine DSFA: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711)

- Klare Prozessdefinition mit Templates/Arbeitshilfen unerlässlich
- Die Integration mit dem ISMS (Risikoanalyse) ist sinnvoll
- Der DSB ist nicht in Durchführungsverantwortung, sondern nur verpflichtend beratend (vor allem beim „Ob“)

Ausblick: Arbeitshilfe von bvitg, DKG und GMDS in Abstimmung

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Fazit

- Manuelle und automatisierte Verarbeitungs-tätigkeiten sind möglichst umfassend zu dokumentieren

- Hohe Risiken sind zu vermeiden bzw. zu vermindern

- Bei „klassischen Datenschutzrisiken“ (Video, GPS, CRM / KIS etc.) sind unabhängig von der Risiko-bewertung des Verantwortlichen auf jeden Fall Datenschutz-Folgeabschätzungen angeraten

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Haben Sie dazu noch Fragen ?