Datenschutzfolgenabschätzung

Ein Werkzeugkoffer

1

Kontakt info@letter-consulting.de

www.5medical-management.de

Tel: 02131 1331166

- Auszug Vita Michael Letter
- Studium Betriebswirtschaft GH Duisburg
- Gründung der 5medical management GmbH 1996
- Seit 15 Jahren im Bereich Datenschutz spezialisiert
- Mitautor der GDD Praxishilfen und der GMDS – Ratgeber
- Referent zum Thema DSFA

2

Agenda

- Kurze Beleuchtung des Art. 35 DS-GVO
- Wann ist eine DFSA durchzuführen?
  - Blacklists der Aufsichtsbehörden
  - LDA Bayern
- Beispiele aus dem medizinischen Umfeld
- Forschung und DSFA
  - Forschungsprivileg und Dokumentation
  - Auffassung LDI Rheinland-Pfalz
  - Checkliste Forschung
- Grundsätze bei einer DSFA
  - Ggf. kurzer Exkurs Drittlandtransfer
- DSFA welche Tools
  - Beispiel mit der GMDS Risikomatrix
  - Praktische Tipps mit der PIA (CNIL)
- Fragerunde

3

Hinweis

- Die Präsentation wird zur Verfügung gestellt
- Pause 10:30 bis 11:00 Uhr
- Vortrag bis ca. 11.45 im Anschluss allgemeine Fragen und Diskussion
- Inhaltliche Fragen, gern auch zwischendurch

4

Welche Erfahrungen haben Sie mit der DSFA?

5

Wann ist dieser Workshop für Sie ein voller Erfolg?

6

Die Rechtsgrundlage Art. 35 DS-GVO

7

Art. 35 DSGVO

Hat 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 Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

8

Art 35 DSGVO

- Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

- a) 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 ähnlich erheblicher Weise beeinträchtigen;

- b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10

- c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

→ Scoring durch Banken, Versicherungen oder Auskunfteien

→ Beispiele folgen

→ Fahrzeugdaten im großen Stil, um freie Parkplätze anzuzeigen

9

Art. 35 DSGVO

Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

z. B. für Forschungszwecke oder Zwecke der Verarbeitung die sehr ähnlich oder gleichgelagert sind.

Achtung Begründung dokumentieren.

10

Art 35 DSGVO

Bitte beachten Sie

- Datenschutzbeauftragte*r ist nur Berater
- Formelle Vorgaben bzgl. Inhalts, was beschrieben werden muss
- Abs. 8 Verhaltensregeln (siehe auch Art. 40 DS-GVO)
- Abs. 9 Standpunkt der Betroffenen
- Abs. 4,5,10 Ausnahmen (Black/Whitelists)
- Abs. 11 PDCA-Zyklus

11

Art 35 DSGVO

Bitte beachten Sie

- Datenschutzbeauftragte*r ist nur Berater
- Formelle Vorgaben bzgl. Inhalts, was beschrieben werden muss
- Abs. 8 Verhaltensregeln (siehe auch Art. 40 DS-GVO)
- Abs. 9 Standpunkt der Betroffenen
- Abs. 4,5,10 Ausnahmen (Black/Whitelists)
- Abs. 11 PDCA-Zyklus

- Hinweis öffentlicher Bereich Länderregelungen
- Kirchen §35 DSG-EKD und §35 KDG

12

5 medical management

DSK
DATENSCHUTZKONFERENZ

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
1	Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: • Daten zu schutzbedürftigen Betroffenen • Systematische Überwachung • Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen • Bewerten oder Einstufen (Scoring) • Abgleichen oder Zusammenführen	Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke.	Ein Unternehmen setzt flächendeckend Fingerabdrucksensoren zur Zutrittskontrolle für bestimmte Bereiche ein. Eine Schulkantine bietet den Schülern das „Bezahlen per Fingerabdruck" an.

Blacklist der Aufsichtsbehörden

- https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf
- https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf

13

5 medical management

Bayerisches Landesamt für Datenschutzaufsicht

BayLDA Online-Services Datenschutz Veröffentlichungen Unsere Behörde Suche...

Datenschutz > Themen > Datenschutz-Folgenabschätzung

Datenschutz-Folgenabschätzung

https://www.lda.bayern.de/de/thema_dsfa.html

Durchführung einer Datenschutz-Folgenabschätzung gem.
Art. 35 DSGVO auf der methodischen Grundlage eines standardisierten
Prozessablaufes mit Rückgriff auf das SDM am
Beispiel eines „Pay as you drive"-Verfahrens (V 0.10)

14

Wann ist eine DSFA durchzuführen?

Umfangreiche Verarbeitung von Daten Artikel 9 Absatz 1

- Einzelpraxis - Nein
- Praxis mit 2 Behandlern - eher Nein
- Praxis mit 2 Inhabern und 5-6 angestellten Ärzten - eher Ja
- Medizinisches Versorgungszentrum mit einer gemeinsamen Anmeldung, ggf. gemeinsamen Abrechnungssystem - Ja

15

Eine DSFA ist durchzuführen

- Krankenhausinformationssystem
- Anonymisierung von besonderen personenbezogenen Daten z. B.
  - Übermittlung an nicht-gesetzlich geregelte Krankheitsregister (Krebsregister)
- Forschung
- Verarbeitung von Art. 9 Daten bei Telemedizin-Anwendungen (Videosprechstunde)
- Verarbeitung von Art. 9 Daten durch zentrale Internetdienste z.B.
  - Verarbeitung von Gesundheitsdaten in der Cloud
  - institutionsübergreifende Patientenakten (z. B. Klinik + Strahlentherapie)
- Offen “ePA; KIM etc.”

16

Exkurs
Forschung und DSFA

17

Forschungsprivileg DSGVO, BDSG, ggf. Landesgesetzte

- Zulässigkeit = DSGVO (allerdings ist dort Forschung nicht definiert)
  ⟶ Rechtsgrundlagen Art 6
  in Verbindung mit Art 9 Gesundheitsdaten
- Transparenzpflichten Art 5 (Nachweise, Dokumentation)

- BDSG-neu §27 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken (Einschränkung der Betroffenenrechte (Art, 15,16,18 und 21)

- LKG Rheinland-Pfalz § 37 Datenschutz bei Forschungsvorhaben (Einwilligungen)

18

Forschungsprivileg DSGVO, BDSG, ggf. Landesgesetzte

- Transparenzpflichten Art 5.2 (Nachweise, Dokumentation, Rechenschaftspflicht)
- Wie beschreibt u. a. Art. 30 Verarbeitungsübersicht (VVT)

- Daraus folgt = Forschungsprojekte sind ins VVT aufzunehmen
- ggf. können gleichlautende Studien oder gemeinsame Studien zusammengefasst werden. (Begründung liefern)

- Die Rechenschaftspflicht bedingt eine Dokumentation und Art. 35 DSGVO die Durchführung einer Datenschutzfolgenabschätzung (Blacklist der DSK)

19

- Checkliste Forschung_DSGVO_2.8.pdf

Rae Marc Rüdlin, Hamburg

Checkliste

Datenschutzbelange bei Forschungsprojekten

Bezeichnung des Forschungsprojekts:			
Kurzbeschreibung:			
Voraussichtlicher Beginn des Forschungsprojekts:		**Voraussichtliches Ende des Forschungsprojekts:**	

	Rechtsgrundlage	Ja	Nein	Anmerkungen
1. Grundrechtsprüfung				
Benötigt das Forschungsvorhaben Patientendaten?	EG 159 zur DSGVO	☐	☐	
Keine unangemessene Beeinträchtigung des Patienten durch Bedarf an Patientendaten?	Art. 2 Abs. 1 GG	☐	☐	

Senden Sie mir eine Mail mit dem Stichwort „Checkliste Forschung“

20

Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz

Prof. Dr. Dieter Kugelmann

Auffassung

- Bei der Forschung im medizinischen Bereich ist eine Datenschutzfolgenabschätzung gemäß Art. 35 DS-GVO unerlässlich.

21

Arbeits- und Praxishilfen

- Arbeitshilfe der GMDS zur Pseudonymisierung/Anonymisierung vom 29. Juni 2018 https://gesundheitsdatenschutz.org/html/pseudonymisierung_anonymisierung.php
- Die Praxishilfe „Datenschutz bei Klinischen Studien“ (https://gesundheitsdatenschutz.org/html/klin_studien.php, Stand 10. Dezember 2019) Für Forscher interessant, auch wenn Anonymisierung nur sehr kurz erwähnt wird. Aber datenschutzrechtliche Anforderungen für medizinische Forscher wurden gut dargestellt.
- Die Praxishilfe „Klinische Register und Datenschutz“ (https://gesundheitsdatenschutz.org/html/klin_register.php, Stand 13. Dezember 2019) betrifft medizinische Forschung eigentlich nur indirekt, aber Kapitel 12.5 betrifft die Anonymisierung. Auch wenn es kurz ist, könnte Abschnitt 12.5.1 von Interesse sein.

22

Praxis Tipp

In der Forschung kann man sehr viel falsch machen.

Bei der Frage zur Anonymisierung ist es oft richtig ihre zuständige Aufsichtsbehörde anzusprechen.

23

Exkurs Drittlandtransfer

- GDD / Bitkom etc. empfehlen Risikobetrachtung/TIA
- EuGH Schrems II „Betroffenenrechte gewährleisten im Drittland“
- Risiko außerhalb der EU betrachten z. B. USA 2018 Cloud Act „Clarifying Lawful Overseas Use of Data Act“

24

Exkurs Drittlandtransfer mögliche Betrachtung

- Risikobetrachtung z. B. betrachten wie wahrscheinlich ist ein Zugriff nach dem Cloud Act – auf med. Daten von Michael Letter in einem Kreiskrankenhaus

  – höchst unwahrscheinlich

- Bei medizinischen Daten von einem Minister in der Charité in Berlin, kann sich ein anderes Ergebnis herausstellen.

- **Hinweis -** keine Aufsicht hat sich bisher dazu geäußert, ob eine DSFA einer Datentransferanalyse ähnlich ist. (Ein zu betrachtendes Risiko ist das Rechtssystem)

- Sie haben bestmöglich das Risiko betrachtet und ihre Entscheidung abgewogen

25

Exkurs MS 365 Azure etc.

- DSK Beschluss zu MS 365
- Seitens MS Zusicherung EU-Datenraum
- Kauf der Lizenz durch IT-Haus
  - AVV Art 28 – Unterauftragnehmer MS-Irland
  - TIA durch IT-Haus oder MS?????
- Ab Mitte 2023 ggf. Angemessenheitsbeschluss EU ??????

26

Exkurs MS 365 Azure etc.

- 2 Checklisten
- Checkliste datenschutzfreundliche Inbetriebnahme von MS 365
- MS 365 aus datenschutzrechtlicher Sicht
- Anfordern unter : info@letter-consulting.de

27

Exkurs Drittlandtransfer mögliche Betrachtung

- Tipp: Datenschutz Praxis (Jana Thieme-Hermann)
- https://www.datenschutz-praxis.de/verarbeitungstaetigkeiten/transfer-impact-assessment-tia-die-einzelfallbewertung/

28

Dr. Bernd Schütze

TIPP

- Seminar 5 „Drittstaatenverarbeitung“
- Referent: Dr. Bernd Schütze
- Seminarunterlagen anfordern

29

Grundsätze der Datenschutzfolgenabschätzung

30

Generell

- Die DSFA muss in der Regel bereits vor der Einführung des Verarbeitungsverfahrens durchgeführt und danach in regelmäßigen Abständen wiederholt werden.
- Der Zweck und die Rechtsgrundlage sind zu beschreiben. Dabei sollte jeweils möglichst konkret vorgegangen werden.
- Darauf folgt eine Bewertung des Risikos für die Rechte und Freiheiten der betroffenen Personen.
- Weiterhin ist eine Prüfung der Verhältnismäßigkeit bezüglich des Verhältnisses der Zwecke zu den datenschutzrechtlichen Risiken erforderlich.

31

Generell

- Auf der Grundlage der Risikobewertung müssen die Sicherheitsmaßnahmen, definiert werden.
- Ggf. andere Akteure einschalten (Datenschutzaufsicht, Betroffene bzw. Vertreter)
- Soweit möglich personenbezogene Daten anonymisieren

32

Generell

- Auf der Grundlage der Risikobewertung müssen die Sicherheitsmaßnahmen, definiert werden.
- Ggf. andere Akteure einschalten (Datenschutzaufsicht, Betroffene bzw. Vertreter)
- Soweit möglich personenbezogene Daten anonymisieren
- **Argumentieren Sie aus der Sicht der Betroffenen**
- **Evaluation meine Erfahrung alle 2-3 Jahre**

33

DSFA durchführen mit..

Nur einige Möglichkeiten

- Das Standard-Datenschutzmodell
file:///C:/Users/admin/Documents/Meine%20Dateien/SDM-Methode_V2.0a.pdf
- ISO/IEC 29134 "Guidelines for privacy impact assessment" (Stand 2017-06 beuth.de LDA Bayern Herr Sax)
https://www.beuth.de/de/norm/iso-iec-29134/276510955
- Bitcom -Risk Assessment & Datenschutz-Folgenabschätzung
https://www.bitkom.org/sites/default/files/file/import/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf
- **PIA der französischen Aufsichtsbehörde CNIL**
- **Werkzeug der GMDS und bvitg**
- **Parallele Anwendung diverser Werkzeuge**

34

Cookie Einstellungen

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

GMDS Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

Datenschutzhinweise Cookie-Hinweise Impressum Kontakt Sitemap Veranstaltungskalender

Home Veranstaltungen DS-GVO Interpretation DS-GVO Praxishilfen Literatur Nationale Umsetzung GMDS AG DIG Links Hilfe

Beispiel für eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO

Am Beispiel eines Krankenhaus-Informationssystems

Der Umgang mit der Datenschutz-Folgenabschätzung ist bisher in Deutschland weitestgehend unbekannt. Eine auf das Gesundheitswesen ausgerichtete Praxishilfe wurde erarbeitet und basierend auf dieser Praxishilfe soll das vorliegende Beispiel eine Hilfestellung bieten, wie eine Datenschutz-Folgenabschätzung umgesetzt werden kann.

Dieses Beispiel besteht aus verschiedenen Teilen:

1. Eine Beschreibung des Beispiel-Krankenhauses und des darin eingesetzten Krankenhaus-Informations-Systems; beides entspringt vollständig der Phantasie, wobei selbstverständlich darauf geachtet wurde, dass die Beschreibung reellen Anwendungen aus der täglichen Praxis entspricht.
2. Eine Umsetzung einer Datenschutz-Folgenabschätzung, basierend auf der beispielhaften Beschreibung. Diese Folgenabschätzung basiert auf zwei Teilen:
   1. Der textuellen Beschreibung der zugrundeliegenden Sachverhalte.
   2. Einer Excel-Tabelle, in welcher die Risiken sowie die Behandlung der Risiken beschrieben werden.

   In der Excel-Tabelle können aus Platzgründen die technisch-organisatorischen Maßnahmen nicht vollumfänglich beschrieben werden; die Übersicht ginge verloren, wenn dies in der tabellenhaften Darstellung erfolgen würde. Daher wurde die ausführlichere Beschreibung dieser Maßnahmen in den Anhang der textuellen Beschreibung eingefügt.

Eine Datenschutz-Folgenabschätzung soll gemäß Art. 35 Abs. 7 lit. a DS-GVO eine „eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung“ beinhalten. Dies beinhaltet natürlich nicht, dass alles von Grund auf erklärt werden muss; in der Praxis gelebte und anerkannte Verfahren bedürfen keiner Erklärung. Zum Beispiel kann davon ausgegangen werden, dass bekannt ist, was unter einer medizinischen Untersuchung zu verstehen oder was HL7 ist. Auch diejenigen, die eine Datenschutz-Folgenabschätzung lesen und ggf. beurteilen, müssen die entsprechende Fachkenntnis aufweisen, zumindest in dem Rahmen, wie man es bei auch bei einem Datenschutzbeauftragten entsprechend den Vorgaben von Art. 37 Abs. 5 DS-GVO („auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens“) erwarten kann.

Eine systematische Beschreibung des geplanten Verarbeitungsvorgangs erfordert eine Erläuterung

- des Datenverarbeitungsprozesses,
- der hierfür eingesetzten Technik sowie
- Art, Umfang und Umstände der Datenverarbeitung.

Und dies erfolgte in Teil 2 in der textuellen Komponente.

Die Ausarbeitung wurde unter einen Creative Commons-Lizenz (4.0 Deutschland Lizenzvertrag) veröffentlicht. Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite https://creativecommons.org/licenses/by-sa/4.0/deed.de bzw. für den vollständigen Lizenztext auf die Webseite https://creativecommons.org/licenses/by-sa/4.0/legalcode.

Download der Ausarbeitung:

(Stand: 2019-12-14)

- Beispiel-DSFA, textuelle Form (pdf-Datei)
- Beispiel-DSFA, Risikodarstellung (Excel-Tabelle)
- Vorlage für eine DSFA (Word, docx)
- Vorlage für die Risikoanalyse bei einer DSFA (Excel-Tabelle, xlsx)
- Vorlage für die Risikoanalyse bei einer DSFA (Excel-Vorlage, xltx)
- Erläuterungen für die word- und Excel-Vorlage (pdf-Datei)

35

Download der Ausarbeitung:

(Stand: 2019-12-14)

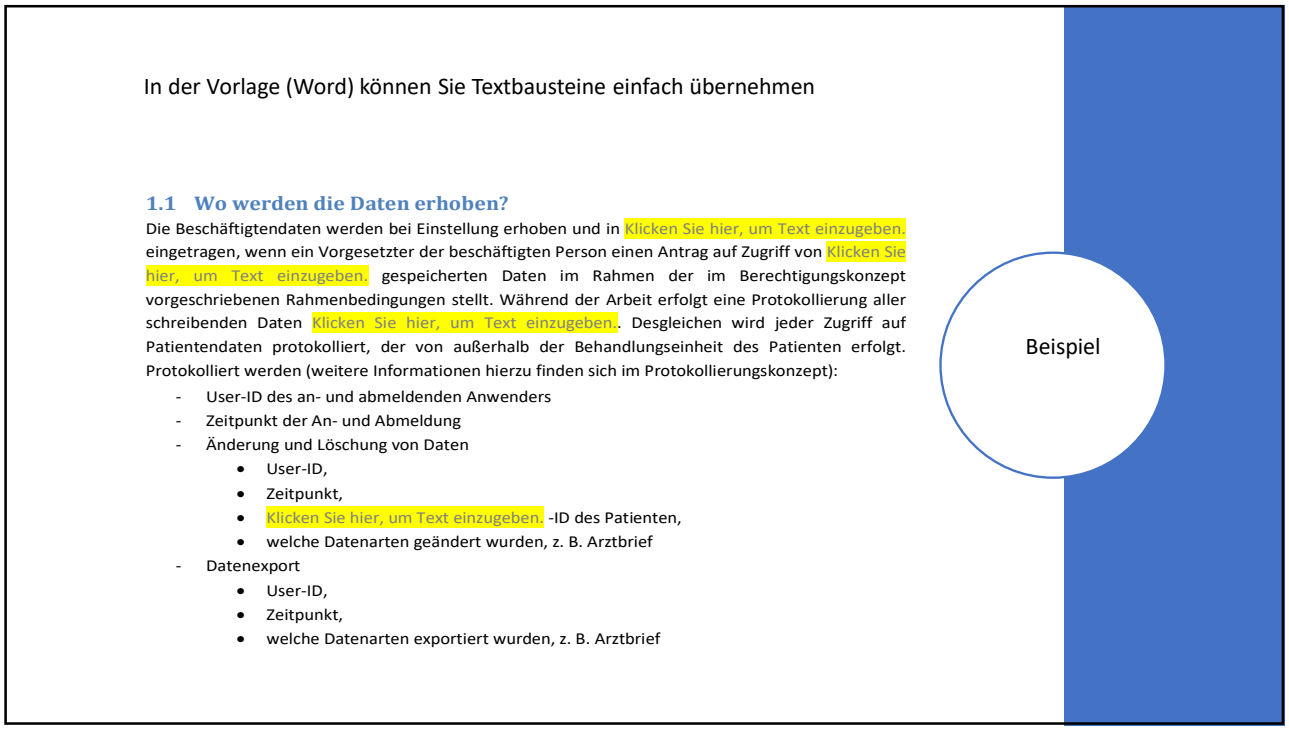
- Beispiel-DSFA, textuelle Form (pdf-Datei)
- Beispiel-DSFA, Risikodarstellung (Excel-Tabelle)
- Vorlage für eine DSFA (Word, docx)
- Vorlage für die Risikoanalyse bei einer DSFA (Excel-Tabelle, xlsx)
- Vorlage für die Risikoanalyse bei einer DSFA (Excel-Vorlage, xltx)
- Erläuterungen für die word- und Excel-Vorlage (pdf-Datei)

https://gesundheitsdatenschutz.org/html/dsfa-beispiel.php

36


Beispielhafter Umgang mit der Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) Am Beispiel eines Krankenhaus-Informationssystems
Eine Zusammenarbeit von
Bundesverband Gesundheits-IT e. V.
Arbeitsgruppe Datenschutz & IT-Sicherheit
bvitg
Bundesverband Gesundheits-IT
Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
gmds
Arbeitskreis „Datenschutz und IT-Sicherheit im Gesundheitswesen"
Autoren
Sabine Fock Klinikum und Seniorenzentrum Itzehoe
Christoph Isele Cerner Deutschland GmbH
Pierre Kaufmann
Michael Letter 5medical management GmbH
Mark Rüdlin Rechtsanwalt + Datenschutzbeauftragter
Jörg Schecker Agfa HealthCare GmbH
Bernd Schütze Deutsche Telekom Healthcare and Security GmbH
Stefan Wunschel Sana Kliniken AG
Idee für eine Dokumentation

37


In der Vorlage (Word) können Sie Textbausteine einfach übernehmen
1.1 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
Beispiel

38

medical management

Tipps

- Aufsichtsbehörde konsultieren Art 36 DS-GVO
- Die Beteiligten zu aktiven Teilnehmern machen
  - ➢ Vorstände/Geschäftsleitungen/etc. mitnehmen
- Mögliche Argumente:
  - ➢ Planspiel, es geht auch um die Assets des Unternehmens, der Klinik oder Praxis
  - ➢ es ist eine Vorsorge, wie eine Art Versicherung

39

medical management

Live Beispiel einer Risikobewertung für eine Datenschutzfolgenabschätzung

Verarbeitungstätigkeit:						Riskoanalyse VOR Maßr			
lfd. Nr.	Risiko-ursprung	Risiken	Risikobeispiele	Risiko-quellen	Risiko-verantwort-licher	Schadens-höhe	Eintritts-wahrschein-lichkeit	Risiko-bewertung	Risiko-bewäl-tigung
		nach Erwägungsgrund 83 DS-GVO				- Niedrig - Normal - Hoch - Sehr hoch	- Niedrig - Mittel - Hoch	- Kein Risiko - Voraussichtlich kein Risiko - (Normales) Risiko	Risiko-vermeidung, minimierung, handhabung,
		Bitte Auswahl anklicken	Bitte Auswahl anklicken	Bitte Auswahl anklicken	Freitext	Bitte Auswahl anklicken	Bitte Auswahl anklicken	Kennzeichnung folgt automatis	Bitte Auswahl anklicken
2.	Allgemein	Informationsfehlerhaftigkeit	Unbefugtes Eindringen in IT-Systeme	Hacker, Lust am „Spielen“		Normal	Niedrig		Risikominimierung
3.	Allgemein	Informationsfehlerhaftigkeit	Schadprogramm	Software, Schaden		Hoch	Hoch		Risikominimierung
4.	Allgemein	Verlust personenbezogener Daten	Diebstahl von Geräten, Datenträgern und Dokumenten	Hardware, Verlust		Hoch	Mittel		Risikominimierung
5.	Allgemein	Veränderung personenbezogener Daten	Manipulation von Informationen	Beschäftigter, Fahrlässigkeit		Hoch	Niedrig		Risikominimierung
6.	Allgemein	Unbefugter Zugang zu personenbezogenen Daten	Offenlegung schützenswerter Informationen	Hacker, Finanzieller Vorteil		Hoch	Mittel		Risikominimierung
7.	Allgemein	Unbefugte Offenlegung personenbezogener Daten	Offenlegung schützenswerter Informationen	Beschäftigter, Vorsatz		Hoch	Niedrig		Risikominimierung
8.	Allgemein	Dauerhafte Verfügbarkeit (negativer) Informationen	Missbrauch personenbezogener Daten	Journalisten, Informationen für Story		Hoch	Mittel		Risikominimierung
9.	Allgemein	Schamgefühl und Ansehensverlust	Missbrauch personenbezogener Daten	Journalisten, Informationen für Story		Hoch	Mittel		Risikominimierung
10.	Allgemein	Finanziellen Verlust	Offenlegung schützenswerter Informationen	Unbefugte Verarbeitung		Hoch	Mittel		Risikominimierung
11.	Allgemein	Arbeitsrechtlicher Kontext	Offenlegung schützenswerter Informationen	Unbefugte Verarbeitung		Hoch	Mittel		Risikominimierung
12.	Allgemein	Gesellschaftlich-politische Risiken	Missbrauch personenbezogener Daten	Unbefugte Verarbeitung		Hoch	Mittel		Risikominimierung
13.	Allgemein	Diskriminierung	Offenlegung schützenswerter Informationen	Unbefugte Verarbeitung		Hoch	Mittel		Risikominimierung
15.	Aufnahme	Falsche Zuordnung von Daten	Falsche Auswahl eines Patienten in einem Informationssystem	Beschäftigter, Fahrlässigkeit		Hoch	Mittel		Risikominimierung
16.	Aufnahme	Falsche Zuordnung von Daten	Falsches Einlesen der Krankenversichertenkarte	Beschäftigter, Fahrlässigkeit		Hoch	Mittel		Risikominimierung
17.	Behandlung	Falsche Zuordnung von Daten	Falsche Auswahl eines Patienten in einem Informationssystem	Beschäftigter, Übermüdung/Überlastung		Hoch	Mittel		Risikominimierung
18.	Abrechnung	Falsche Zuordnung von Daten	Fehlerhafte Dokumentation/Dateneingabe	Beschäftigter, Fahrlässigkeit		Hoch	Mittel		Risikominimierung
19.	Allgemein	Enttäuschung von Vertraulichkeitserwartungen	Ausfall oder Störung von Kommunikationsnetzen	Hardware, Überlastung: Ausfall Stromversorgung		Normal	Mittel		Risikominimierung
20.								x	
21.								x	
22.								x	
23.								x	
24.								x	
25.								x	
26.								x	
27.								x	
28.								x	
29.								x	
30.								x	

40

- LIVE

https://www.cnil.fr/en/privacy-impact-assessment-pia

AC4BA320.json

41

Diskussion Fragen

42

Vielen Dank

43