Datenschutz-Folgenabschätzung

Dr. Bernd Schütze

Seminar Datenschutz-Grundverordnung (DS-GVO)

HEALTHCARE SOLUTIONS

Was ist eine DSFA?

Datenschutz-Folgenabschätzung (DSFA)

Worum geht es (Kurzfassung)

- Risikomanagement
- Abschätzung des Risikos *für die* von der (Daten-) Verarbeitung *betroffenen* (natürlichen) *Personen*
- Risiko für das die Daten verarbeitende Unternehmen spielen keine Rolle (obgleich diese natürlich motivierend wirken können)
- Minimierung der gefundenen Risiken durch technisch-organisatorische Maßnahmen
- Entscheidung:
  a) Risiko wurde derart minimiert, dass es *aus Sicht der betroffenen Person* akzeptabel ist
  b) Risiko kann nicht derartig minimiert werden
     1) Auf Verarbeitung verzichten
     2) Abstimmung mit zuständiger Aufsichtsbehörde, ob Verarbeitung trotzdem erfolgen kann

Rechtliche Grundlagen

Rechtliche Grundlage
(Artt. 35,36 DS-GVO)

Wann muss eine DSFA durchgeführt werden?

– DSFA muss erfolgen (Art-. 35 DS-GVO)

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 Art. 9 Abs. 1 DS-GVO

c) Umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO

d) Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

e) Immer, wenn die Verarbeitung der personenbezogenen Daten ein hohes Risiko für die Rechte und Freiheiten der Betroffenen birgt
(insbesondere bei Technologien, die vorher noch nicht vom Verantwortlichen eingesetzt wurden)

Rechtliche Grundlage
(Artt. 35,36 DS-GVO)

Wann muss eine DSFA durchgeführt werden?

- Deutsche Aufsichtsbehörden veröffentlichten Kriterienlisten, wann aus ihrer Sicht eine DSFA erforderlich ist
- Für den Gesundheitssektor sind insbesondere von Interesse
  - Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Weiterverarbeitung der so zusammengeführten Daten
    (z.B. Big Data, Data-Warehouse)
  - Erhebung personenbezogener Daten über Schnittstellen persönlicher elektronischer Geräte, die nicht gegen ein unbefugtes Auslesen geschützt sind
    (z.B. Einsatz von Tracking mittels RFID-Chips)
  - Anonymisierung von besonderen personenbezogenen Art. 9 Daten
  - Verarbeitung von Art. 9 Daten sofern eine nicht einmalige Datenerhebung mittels Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden
    (z.B. Telemedizin-Anwendungen)
  - Verarbeitung von Art. 9 Daten durch zentrale Internetdienste
    (z.B. Verarbeitung von Gesundheitsdaten in der Cloud, institutionsübergreifende Pat.-Akten)

Rechtliche Grundlage
(Artt. 35,36 DS-GVO)

Was sind die (Mindest-) Inhalte?

- Eine *systematische Beschreibung* der geplanten *Verarbeitungsvorgänge*;
- Eine *systematische Beschreibung* der *Zwecke der Verarbeitung*, ggf. einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- Eine *Bewertung* der *Notwendigkeit und Verhältnismäßigkeit* der Verarbeitungsvorgänge in Bezug auf den Zweck;
- Eine *Bewertung der Risiken* für die Rechte und Freiheiten der betroffenen Personen gemäß Art. 35 Abs. 1 DS-GVO;
- Die zur Bewältigung der Risiken geplanten *Abhilfemaßnahmen*, einschließlich

  Garantien, Sicherheitsvorkehrungen und Verfahren,

  durch die der *Schutz personenbezogener Daten sichergestellt* und

  der *Nachweis* dafür *erbracht* wird, dass

  die Anforderungen der DS-GVO eingehalten werden, wobei

  den *Rechten und berechtigten Interessen* der *betroffenen Personen und sonstiger Betroffener* Rechnung getragen wird.

Rechtliche Grundlage
(Artt. 35,36 DS-GVO)

Weitere Anforderungen

- Einbindung des Datenschutzbeauftragten
  (Art. 35 Abs. 2 DS-GVO)
- Ggf. Einholung den Standpunkt der betroffenen Personen oder ihrer Vertreter
  (Art. 35 Abs. 9 DS-GVO)
- Überprüfung durch den Verantwortlichen, ob
  a) Bewertung, ob eine DSFA erforderlich ist, durchgeführt wird und Nachweis(e) dafür vorhanden ist
  b) DSFA ggf. (nachvollziehbar) durchgeführt wird

  (Art. 35 Abs. 11 DS-GVO)
- Rechenschaftspflicht des Verantwortlichen
  (Art. 5 Abs. 2 DS-GVO)

Rechtliche Grundlage
(Artt. 35,36 DS-GVO)

Folgen

- Ggf. Einschaltung Aufsichtsbehörden
  - DSFA ergibt hohes Risiko und
  - Verantwortliche kann/will keine Maßnahmen ergreifen, um Risiko entsprechend zu minimieren

  ➔ Konsultation Aufsichtsbehörde erforderlich
  (Art. 36 Abs. 1 DS-GVO)
- Sanktionen
  - DSFA nicht oder nicht richtig durchgeführt

  ➔ Bußgeld von bis zu „10.000.000 EUR bzw. 2% des weltweiten Umsatzes des Vorjahres
  (Art. 83 Abs. 3 lit. a DS-GVO)

Durchführung einer DSFA

Durchführung einer DSFA

Grundlegendes Vorgehen

- Zusammenstellen des DSFA-Teams und Erarbeitung eines Prüfplanes
- Festlegung des zu betrachtenden Prüfumfangs
- Einbeziehung von DSB und Betroffene / Vertreter
- Bewertung Notwendigkeit und Verhältnismäßigkeit der Daten-verarbeitung
- Feststellen der Rechtsgrundlagen
- Identifizierung und Beurteilung der Risiken
- Prüfung von Abhilfemaßnahmen
- Erstellung eines Berichtes und der Empfehlung zur Umsetzung der Maßnahmen
- Falls erforderlich: Konsultation/Information der Aufsichtsbehörde
- Test der Abhilfemaßnahmen und bei deren Wirksamkeit die Freigabe der Verarbeitung

- Wiederholung der DSFA bei geänderten Risiken
- Regelmäßige Prüfung der Wirksamkeit der Maßnahmen
- Nachweis muss geführt werden

Durchführung einer DSFA

Risikomanagement

- Identifikation der Risiken
- Beschreibung der Risikoart, Ursachen und Auswirkungen
- Analyse der identifizierten Risiken hinsichtlich ihrer Eintrittswahrscheinlichkeiten und möglichen Auswirkungen
  - → *für die Rechte und Freiheiten der betroffenen Person*
- Risikobewertung durch Vergleich mit zuvor festzulegenden Kriterien der Risiko-Akzeptanz
- Festlegung von Maßnahmen, welche Risiken reduzieren oder die Folgen beherrschbar machen
- Risikoüberwachung
- Bei Bedarf: Re-Evaluierung

Durchführung einer DSFA

Dokumentation der DSFA

- Beschreibung des Zweckes bzw. der Zwecke, die mit der Verarbeitung erreicht werden sollen, z.B.
  - Aus- und Weiterbildung
  - Nutzung durch die behandelte Person
  - Forschung
  - Qualitätssicherung
  - Juristische Zwecke
- Begründung, warum die Informationen verarbeitet werden müssen
  - Darstellung der Notwendigkeit der Nutzung der Informationen zur Erreichung der dargestellten Zwecke
- Darstellung des Verarbeitungsvorgangs, insbesondere unter Berücksichtigung
  - Wer verarbeitet welche Daten wann unter welchen Bedingungen welche Daten wozu?
  - Speicherdauer, Löschvorgaben, ...
  - Wahrnehmung Betroffenenrechte
  - Gewährleistung Sicherheit der Daten
- Beschreibung der rechtlichen Grundlage, auf welcher die Verarbeitung erfolgt
  - Einwilligung, gesetzliche Vorschrift, Vertragsverhältnis, ...
- Weitergabe der Daten an Dritte
  - Gesetzliche Vorgaben, Vertragspartner, ...

Durchführung einer DSFA

Risiko-Identifizierung

- Risiken für die betroffenen Personen, z.B.
  1. Strukturelle Risiken
     a) Gesellschaftlich-politische Risiken
     b) Wirtschaftliche Risiken
     c) ...
  2. Individuelle Risiken
     a) Erhöhung individueller Verletzlichkeit für Straftaten
     b) Schamgefühl und Publizitätsschäden
     c) Informationsfehlerhaftigkeit
     d) ...
  3. Risiken für Gesellschaft und Individuum
     a) Behandlung des Menschen als bloßes Objekt
     b) Bildung eines Persönlichkeitsprofils
     c) Fremdbestimmung
     d) ...
  4. ...

Durchführung einer DSFA

Risiko-Bewertung

- Der (potenzielle) Schaden muss klassifiziert werden
- Die Eintrittswahrscheinlichkeit muss abgeschätzt werden, z. B.
  - Hoch: Tritt wahrscheinlich auf, oft, häufig
  - Mittel: Kann auftreten, jedoch nicht häufig
  - Niedrig: Unwahrscheinliches Auftreten, selten, fernliegend
- Basierend auf diesen beiden Ergebnissen wird das Risiko klassifiziert, z. B.
  - Katastrophal: Erhöhung individueller Verletzlichkeit für Straftaten
  - Kritisch: Diskriminierung, Stigmatisierung
  - Ernst: Wirtschaftliche Folgen, Folgen im Berufsleben
  - Gering: Bildung eines Persönlichkeitsprofils
  - Vernachlässigbar: Unannehmlichkeiten
- Bewertung entsprechend Risiko-Matrix, z. B.

  Risiko = Eintrittswahrscheinlichkeit x Schadensklassifikation

Durchführung einer DSFA

Restrisiko-Bewertung

- Ist das unter Berücksichtigung aller getroffenen Maßnahmen bestehende Restrisiko *aus Sicht der betroffenen Personen* akzeptabel?
  - a) Ja
    - ➔ Verarbeitung durchführen
  - b) Nein
    - 1) Verarbeitung nicht durchführen
    - 2) Aufsichtsbehörde kontaktieren. Diese entscheidet:
      - a. Verarbeitung durchführen
      - b. Verarbeitung unterlassen

Arbeitsgruppe: bvitg, DKG, GMDS

Praxishilfe: Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO

Datenschutz-Folgenabschätzung
gemäß Art. 35 DS-GVO

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.

bvitg

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

gmds

Arbeitskreis „Datenschutz und IT-Sicherheit im Gesundheitswesen"

Deutsche Krankenhausgesellschaft e. V.

DEUTSCHE KRANKENHAUS GESELLSCHAFT DKG

Autoren

Ina Haag	Deutsche Krankenhausgesellschaft e.V.
Andrea Hauser	Deutsche Krankenhausgesellschaft e.V.
Christoph Isele	Cerner Deutschland GmbH
Lukas Mempel	Sana Kliniken AG
Christoph Nahrstedt	Nuance Communications
Jan Neuhaus	Deutsche Krankenhausgesellschaft e.V.
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Gerald Spyra	Ratajczak und Partner mbB Rechtsanwälte
Stefan Wunschel	Sana Kliniken AG

Stand: 10.04.2018

Gemeinsame Praxishilfe von bvitg, DKG und GMDS

Stand: 2018-04

Download unter http://ds-gvo.gesundheitsdatenschutz.org/download/dsfa_2018-04-10.pdf

DSFA und Normen

DSFA und Normen

ISO/IEC DIS 29134 „Privacy impact assessment - Guidelines“

- Wann ist
- Einbindu
- Durchfüh
- Follow-U
- Anhang, Personer

Supporting assets	Action	Privacy risk	Examples of threats
Hardware	Abnormal use	Disappearances of PII	Storage of personal files; personal use, etc.
Hardware	Abnormal use	Illegitimate accesses to the PII	Use of USB flash drives or disks that are ill-suited to the sensitivity of the information; use or transportation of sensitive hardware for personal purposes, etc.
Software	Loss	Disappearances of PII	Non-renewal of the license for software used to access data, etc.
Software	Modification	Disappearances of PII	Errors during updates, configuration or maintenance; infection by malware; replacement of components, etc.
Computer channels	Espionage	Illegitimate accesses to the PII	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc.
Computer channels	Loss	Disappearances of PII	Theft of copper cables, etc.
Individuals	Abnormal use	Unwanted changes in the PII	Influence (rumor, disinformation, etc.), etc.
Individuals	Loss	Illegitimate accesses to the PII	Employee poaching; assignment changes; takeover of all or part of the organization, etc.
Paper documents	Damage	Disappearances of PII	Aging of archived documents; burning of files during a fire, etc.
Paper documents	Modification	Unwanted changes in the PII	Changes to figures in a file; replacement of an original by a forgery, etc.

ler auch

z-Grundverordnung (DS-GVO)

Sicherheit der Verarbeitung

Nutzung von Normen

DIN 27799

Contents

DIN 27002

6.2.2 Telearbeit

Maßnahme

Eine Richtlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Information, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden, sollten umgesetzt sein.

Anleitung zur Umsetzung

Organisationen, die Telearbeit erlauben, sollten eine Richtlinie zur Definition von Bedingungen und Einschränkungen für die Nutzung von Telearbeit erlassen. Soweit erforderlich und gesetzlich zulässig, sollten folgende Themen berücksichtigt werden:

a) die bestehende physische Sicherheit des Telearbeitsstandortes unter Berücksichtigung der physischen Sicherheit des Gebäudes und der lokalen Umgebung;

b) die vorgeschlagene physikalische Telearbeitsumgebung;

c) die Sicherheitsanforderungen für die Kommunikation, unter Berücksichtigung des notwendigen Fernzugriffs auf interne organisationseigene Systeme, die Sensibilität der Information auf die zugegriffen und die über Telekommunikationsverbindungen weitergegeben wird sowie die Empfindlichkeit der internen Systeme;

d) die Bereitstellung von virtuellen Desktop-Zugriffen, der Verarbeitung und Speicherung von Information auf privaten Geräten unterbindet;

e) die Gefahr des unbefugten Zugriffs auf Information durch andere Personen in derselben Unterkunft, z. B. Familie und Freunde;

f) die Verwendung von Heimnetzwerken und Anforderungen und Beschränkungen der Konfiguration von drahtlosen Netzwerkdiensten;

g) Richtlinien und Verfahren, um Streitigkeiten über Rechte an geistigem Eigentum zu verhindern, das auf privaten Geräten erarbeitet wurde;

h) Zugang zu Geräten in Privateigentum (um die Sicherheit der Maschine zu überprüfen oder während einer Untersuchung), der von Gesetzes wegen verhindert werden könnte;

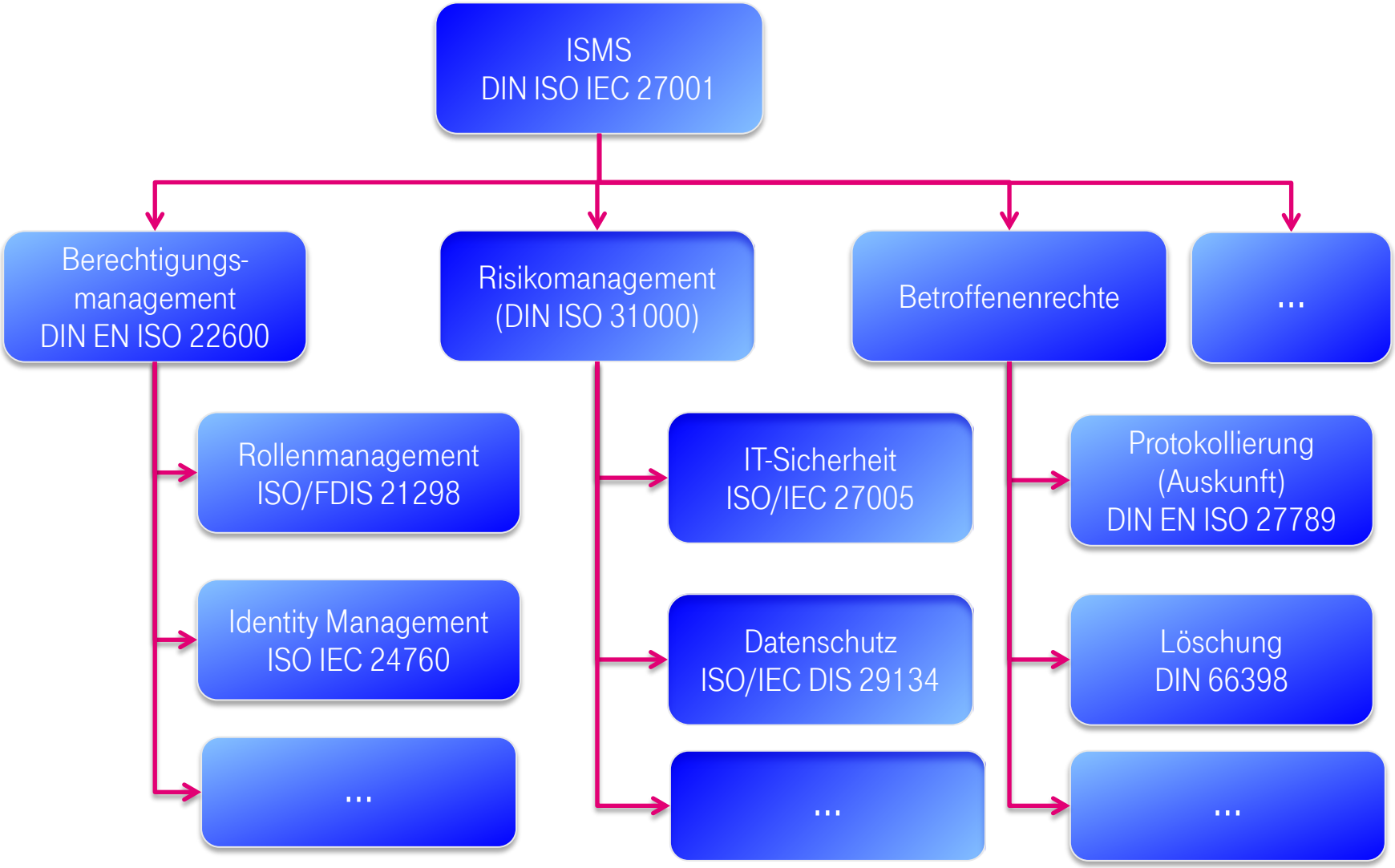
i) Software-Lizenzvereinbarungen, die dergestalt sind, dass Organisationen für die Lizenzierung von Client-Software auf privaten Arbeitsgeräten von Beschäftigten oder sonstiger Benutzer, die zu externen Parteien gehören verantwortlich werden könnten;

j) Anforderungen an Schadsoftwareschutz und Firewall.

Die zu berücksichtigen Richtlinien und Regelungen sollten enthalten:

a) die Bereitstellung geeigneter Geräte und Aufbewahrungsmöbel für Telearbeitstätigkeiten, dort wo der Einsatz von privaten, nicht unter der Aufsicht der Organisation stehenden Geräten untersagt ist;

DSFA UND IT-SICHERHEIT: ZUSAMMENARBEIT



Beispiel

Beispiel bzgl. Umsetzung

Software der CNIL

- Französische Aufsichtsbehörde „ Commission Nationale de l'Informatique et des Libertés“ (CNIL) stellt Software zur Verfügung
- URL: https://www.cnil.fr/en/privacy-impact-assessment-pia