Datenschutz-Folgenabschätzung: Umsetzung am Beispiel eines KIS

Dr. Bernd Schütze

2. Fachtagung „Datenschutz im Gesundheitswesen“

HEALTHCARE SOLUTIONS

Vita

HEALTHCARE SOLUTIONS

Deutsche Telekom Healthcare and Security Solutions GmbH
Dr. Bernd Schütze
Senior Experte Medical Data Security

☎ +49 (160) 9566 - 3145
Bernd.Schuetze@T-Systems.com

Studium

- Informatik (FH-Dortmund)
- Humanmedizin (Uni Düsseldorf / Uni Witten/Herdecke)
- Jura (Fern-Uni Hagen)

Ergänzende Ausbildung

- Datenschutzbeauftragter (Ulmer Akademie für Datenschutz und IT-Sicherheit)
- Datenschutz-Auditor (TüV Süd)
- Medizin-Produkte-Integrator (VDE Prüf- und Zertifizierungsinstitut)

Berufserfahrung

- Über 10 Jahre klinische Erfahrung
- Mehr als 20 Jahre IT im Krankenhäusern
- > 20 Jahre Datenschutz im Gesundheitswesen

Mitarbeit in wiss. Fachgesellschaften

- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)
- Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)
- Gesellschaft für Informatik (GI)

Mitarbeit in Verbänden

- Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)
- Berufsverband Medizinischer Informatiker e.V. (BVMI)
- Fachverband Biomedizinische Technik e.V. (fbmt)
- HL7 Deutschland e.V.
- HE Deutschland e.V.

Agenda

Was ich heute vorstellen möchte

- Kurzfassung: Was ist eine DSFA?
- Rechtliche Grundlagen
- Durchführung einer DSFA
- DSFA und DSK
- DSFA und Normen
- Umsetzungshilfen
  - CNIL
  - Ergebnisse der Arbeitsgruppe von bvitg, DKG, GMDS
- Diskussion/Fragen

Grundsätzlicher Hinweis

Diskussion/Fragen

Virtuelle Seminare stellen besondere Herausforderungen an die Interaktion. Deshalb:

- Einzelne Blöcke sind abgetrennt voneinander
  (graue Trennfolie mit Überschrift des folgenden Blockes)
- Nach jedem Block gibt es Zeit, Fragen zu dem gerade besprochenen Block zu stellen
- Zum Schluss gebt es dann die Gesamtdiskussion

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)

DSFA und DSK

DSFA und DSK

Datenschutzkonferenz: Vorgaben der deutschen Aufsichtsbehörden

- Nationale Aufsichtsbehörden **müssen** eine Liste der Verarbeitungsvorgänge erstellen und veröffentlichen, für die eine DSFA durchzuführen ist (Art. 35 Abs. 4 DS-GVO)
- Aufsichtsbehörden **können** eine Liste der Verarbeitungsvorgänge erstellen und veröffentlichen, für die keine DSFA durchgeführt werden muss (Art. 35 Abs. 5 DS.GVO)

  ➔ Deutsche DSK: es wird keine „Negativliste“ geben
- Vor Festlegung der Listen **muss** Kohärenzverfahren angewendet werden (Art. 35 Abs. 6 DS-GVO), wenn Listen Verarbeitungstätigkeiten umfassen, die
  - mit dem **Angebot von** Waren oder **Dienstleistungen** für **betroffene Personen** oder
  - der Beobachtung des Verhaltens dieser Personen

  in mehreren Mitgliedstaaten im Zusammenhang stehen oder
  - die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten

  ➔ Gilt auch für Gesundheitsdienstleistungen

DSFA und DSK

Datenschutzkonferenz: Vorgaben der deutschen Aufsichtsbehörden

- EDSA: Opinion 5/2018 (Stand: 2018-09-25) on the draft list of the competent supervisory authorities of Germany regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)
  https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art_64_de_sas_dpia_list_de_0.pdf
- Anpassungsbedarf hinsichtlich der eingereichten Liste, geänderter Listenentwurf muss neu eingereicht werden
- DSK passte Liste an, aktuelle Liste Stand 2018-10-17
  https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf
  - Ob geänderte Liste bei EDSA eingereicht wurde, ist unbekannt
    - ➢ Transparenzanforderung aus Art. 5 DS-GVO umgesetzt?
  - Stellungnahme von EDSA zur geänderten Liste liegt nicht vor
    - ➢ Erfüllt die Liste die Anforderungen von Art. 35 Abs. 6 DS-GVO?
    - ➢ Wenn nicht, ist sie dann trotzdem anzuwenden?

DSFA und DSK

DSK: Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

DSFA **muss** bspw. durchgeführt werden:

- Ziff. 2: Verarbeitung von gen. Daten, wenn ein weiteres Kriterium aus WP 248 Rev. 01* zutrifft
  - Z.B. schutzbedürftige Betroffene entspr. ErwGr. 75 DS-GVO
  - Also Betroffene in Situationen, in denen ein ungleiches Verhältnis zwischen der Stellung des Betroffenen und der des für die Verarbeitung Verantwortlichen wie z.B. Kinder, Arbeitnehmer, Patienten, ...
- Ziff. 3: Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs-oder besonderen Amtsgeheimnis unterliegen
- Ziff. 6: Mobile optisch-elektronische Erfassung personenbezogener Daten in öffentlichen Bereichen, sofern die Daten aus ein oder mehreren Erfassungssystemen in großem Umfang zentral zusammengeführt werden.
  - Z.B. telemedizinische Überwachung, wenn die telemed. Daten mit Daten aus PVS, KIS usw. zusammengeführt werden?

* **Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01):** https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

DSFA und DSK

DSK: Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

DSFA **muss** bspw. durchgeführt werden:

- Ziff. 11: Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person
- Ziff. 15: Anonymisierung von besonderen personenbezogenen Daten nach Artikel 9 DS-GVO nicht nur in Einzelfällen zum Zweck der Übermittlung an Dritte
  - Weitergabe z.B. an Krankheitsregister, Forscher, ...
- Ziff. 16: Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist -sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.
  - Telemedizin

* **Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01):** https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

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

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

Sicherheit der Verarbeitung

Nutzung von Normen zur Umsetzung der Risiko-Minimierung

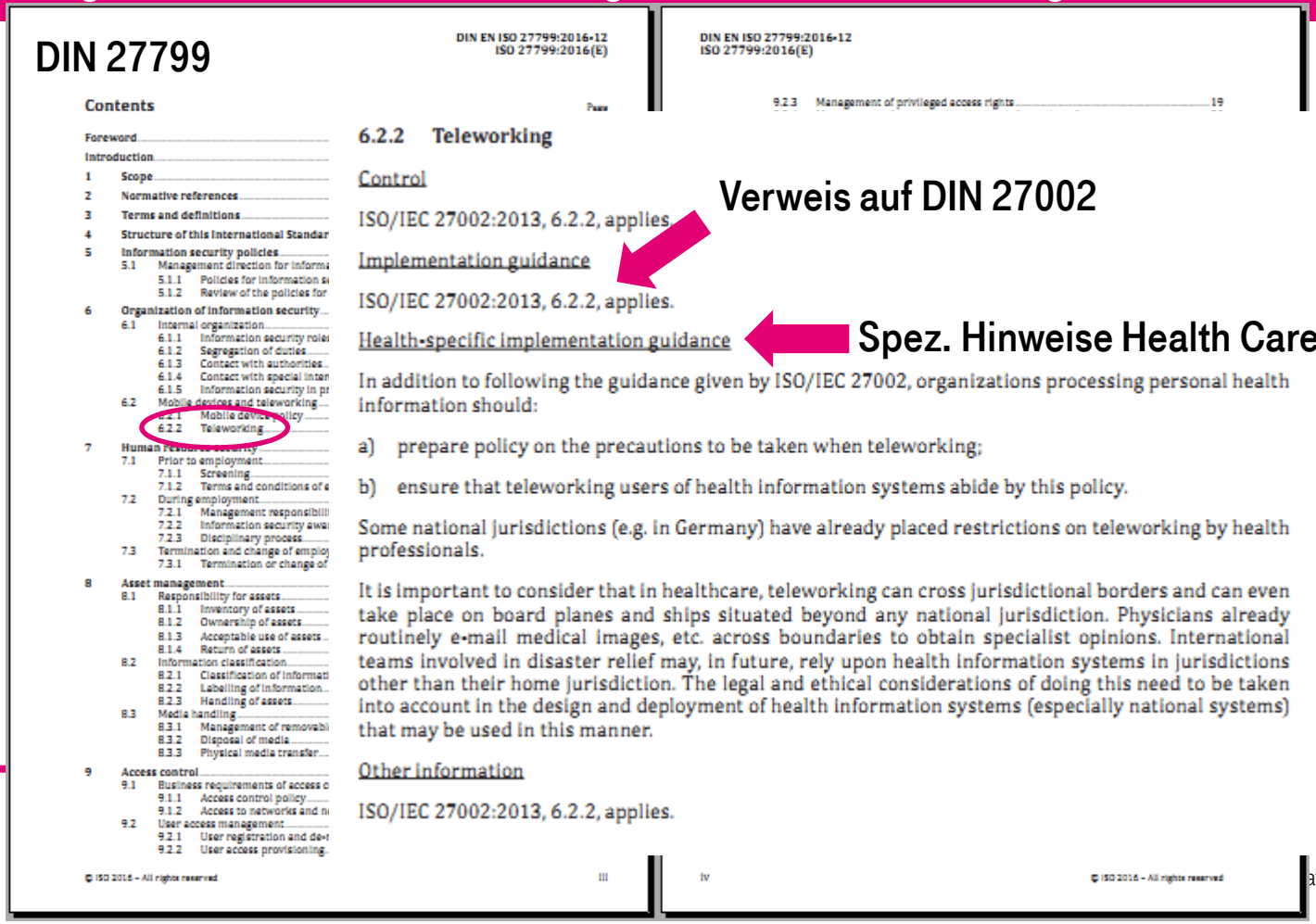
DIN 27799

Contents Page

Sicherheit der Verarbeitung

Nutzung von Normen zur Umsetzung der Risiko-Minimierung

DIN 27799



DIN EN ISO 27799:2016-12
ISO 27799:2016(E)

Contents

DIN EN ISO 27799:2016-12
ISO 27799:2016(E)

6.2.2 Teleworking

Control

ISO/IEC 27002:2013, 6.2.2, applies.

Verweis auf DIN 27002

Implementation guidance

ISO/IEC 27002:2013, 6.2.2, applies.

Health-specific implementation guidance

Spez. Hinweise Health Care

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should:

a) prepare policy on the precautions to be taken when teleworking;

b) ensure that teleworking users of health information systems abide by this policy.

Some national jurisdictions (e.g. in Germany) have already placed restrictions on teleworking by health professionals.

It is important to consider that in healthcare, teleworking can cross jurisdictional borders and can even take place on board planes and ships situated beyond any national jurisdiction. Physicians already routinely e-mail medical images, etc. across boundaries to obtain specialist opinions. International teams involved in disaster relief may, in future, rely upon health information systems in jurisdictions other than their home jurisdiction. The legal and ethical considerations of doing this need to be taken into account in the design and deployment of health information systems (especially national systems) that may be used in this manner.

Other information

ISO/IEC 27002:2013, 6.2.2, applies.

© ISO 2016 – All rights reserved

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;

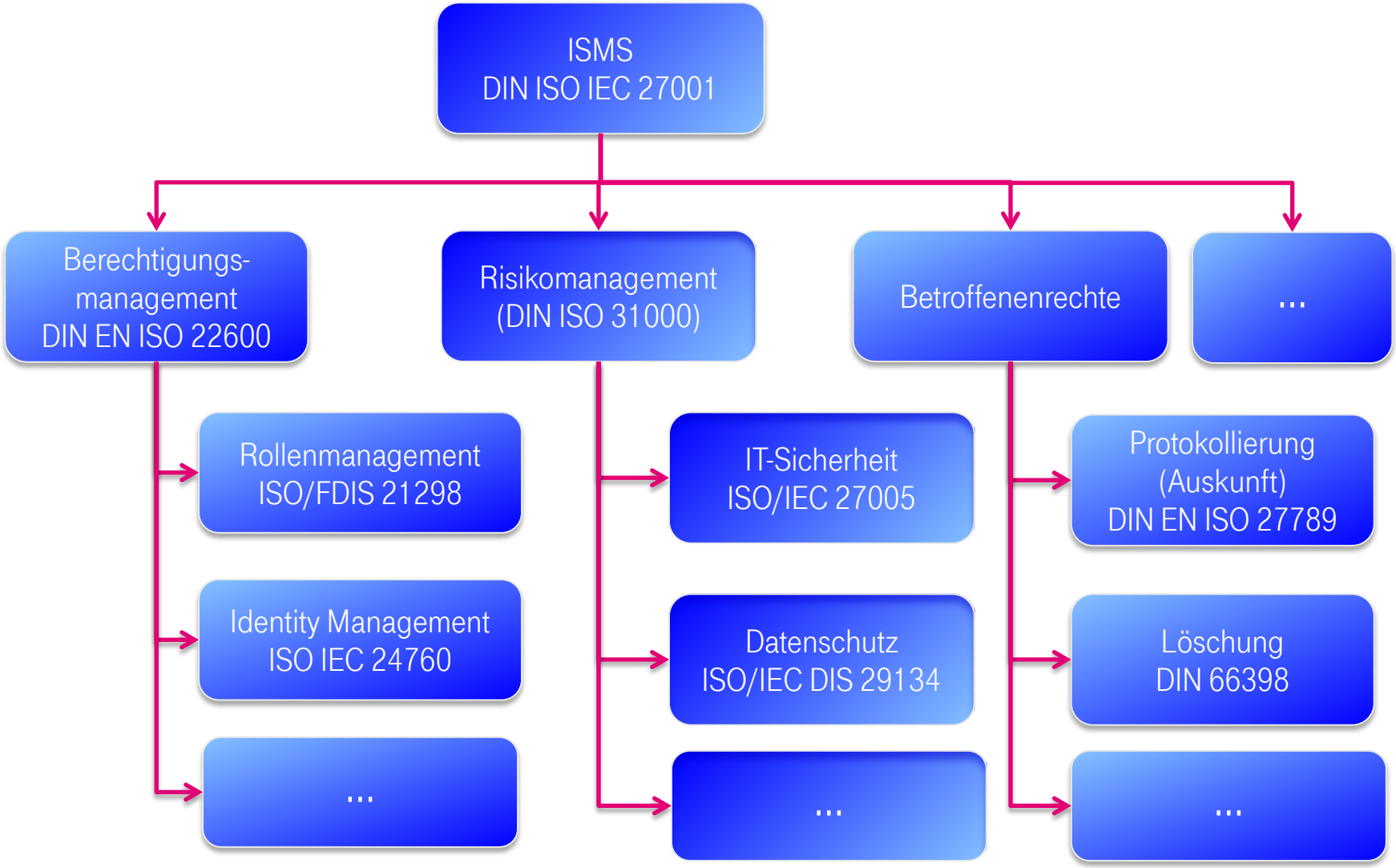
i) Software-Lizenzvereinbarungen, die dergestalt sind, dass Organisationen für die Lizenzierung von Client-Software auf privaten Arbeitsgeräten von Beschäftigten oder sonstiger Benutzer, die zu externen Parteien gehören verantwortlich werden könnten;

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



Umsetzungshilfen: CNIL

Commission Nationale de l'Informatique et des Libertés (CNIL)

Praxishilfen der CNIL

- Französische Aufsichtsbehörde „ Commission Nationale de l'Informatique et des Libertés“ (CNIL) stellt Praxishilfe inkl. Software für Data Protection Impact Assessment (DPIA) zur Verfügung:
  URL https://www.cnil.fr/en/privacy-impact-assessment-pia
  - DPIA Guidelines
    - Infografik zur Durchführung einer DPIA
    - URL: https://www.cnil.fr/en/guidelines-dpia
  - PIA Guides (pdf)
    - Privacy Impact Assessment (PIA) : application to connected objects
    - Privacy Impact Assessment (PIA) 1 : methodology
    - Privacy Impact Assessment (PIA) 2 : template
    - Privacy Impact Assessment (PIA) 3 : knowledge bases
    - URL: https://www.cnil.fr/en/PIA-privacy-impact-assessment-en

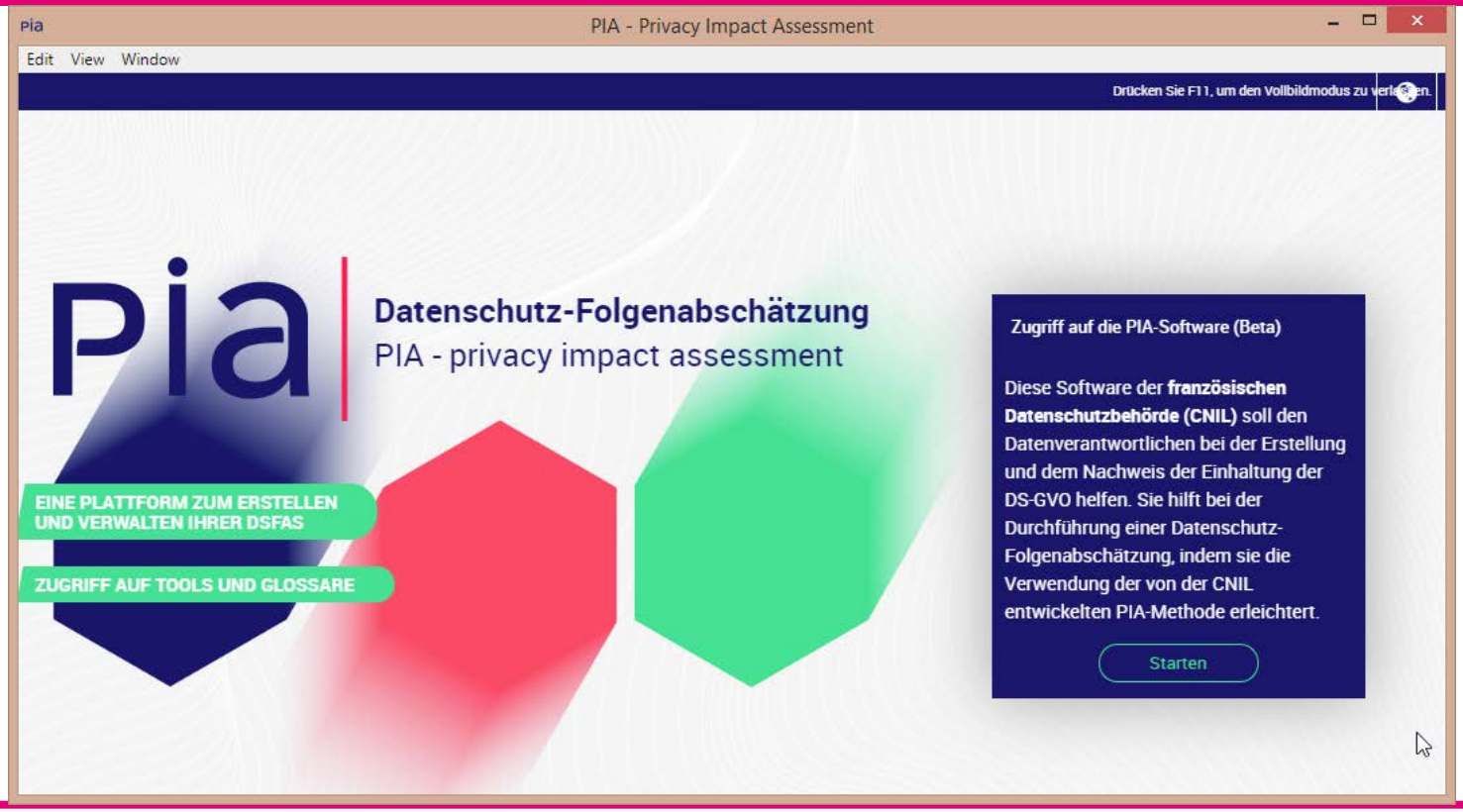
Commission Nationale de l'Informatique et des Libertés (CNIL)

Praxishilfen der CNIL

- Französische Aufsichtsbehörde „ Commission Nationale de l'Informatique et des Libertés“ (CNIL) stellt Praxishilfe inkl. Software für Data Protection Impact Assessment (DPIA) zur Verfügung:
  URL https://www.cnil.fr/en/privacy-impact-assessment-pia
  - Software
    - Portable Version
      - ✓ Einzelplatzrechner
    - Web-Version
      - ✓ Intranet (idealerweise Linux-Server mit Apache, PostgresSQL)
      - ✓ Grundlage Server: Ruby on Rails and Angular JS
    - Tutorial (YouTube)
    - https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

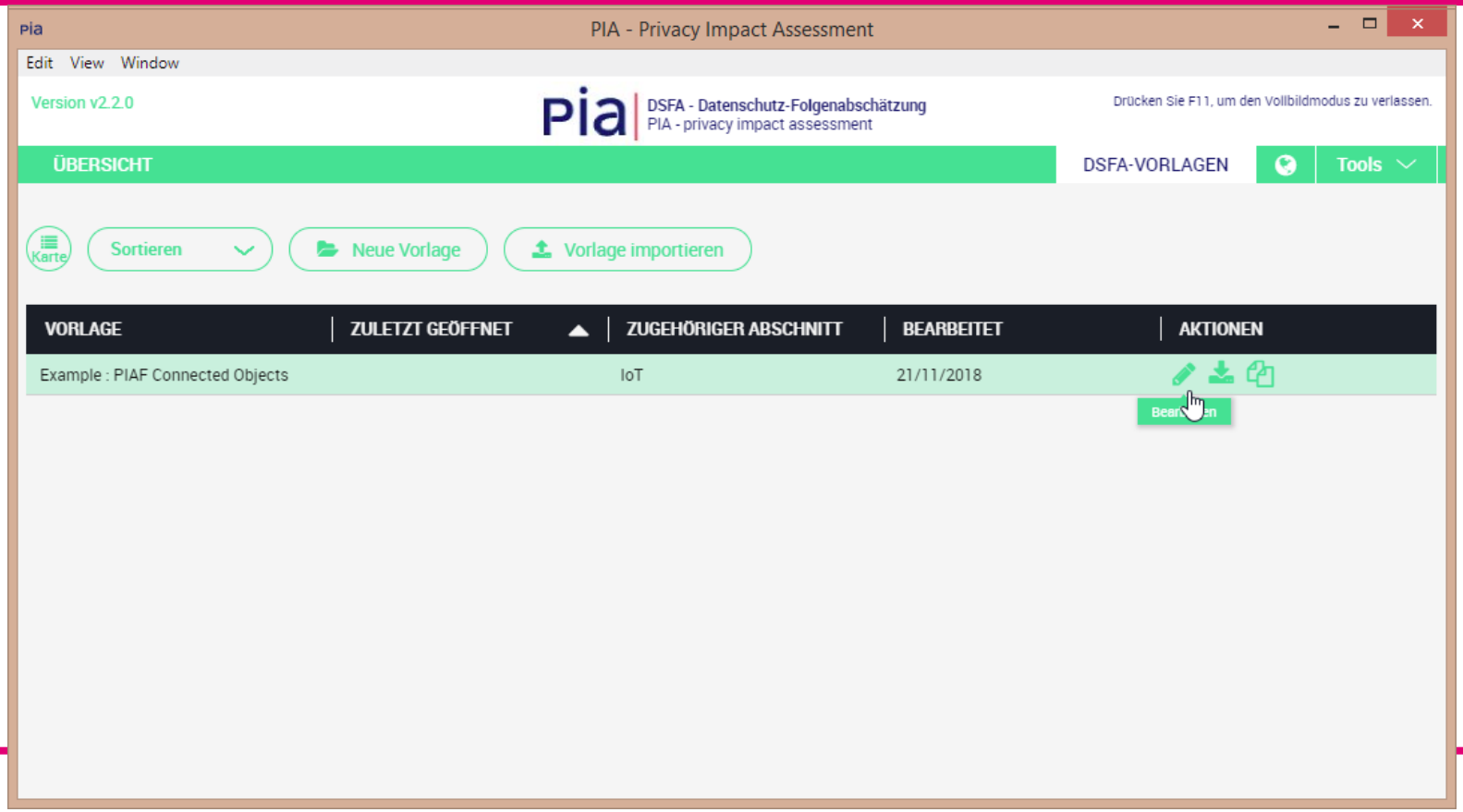
Beispiel bzgl. Umsetzung

Software der CNIL



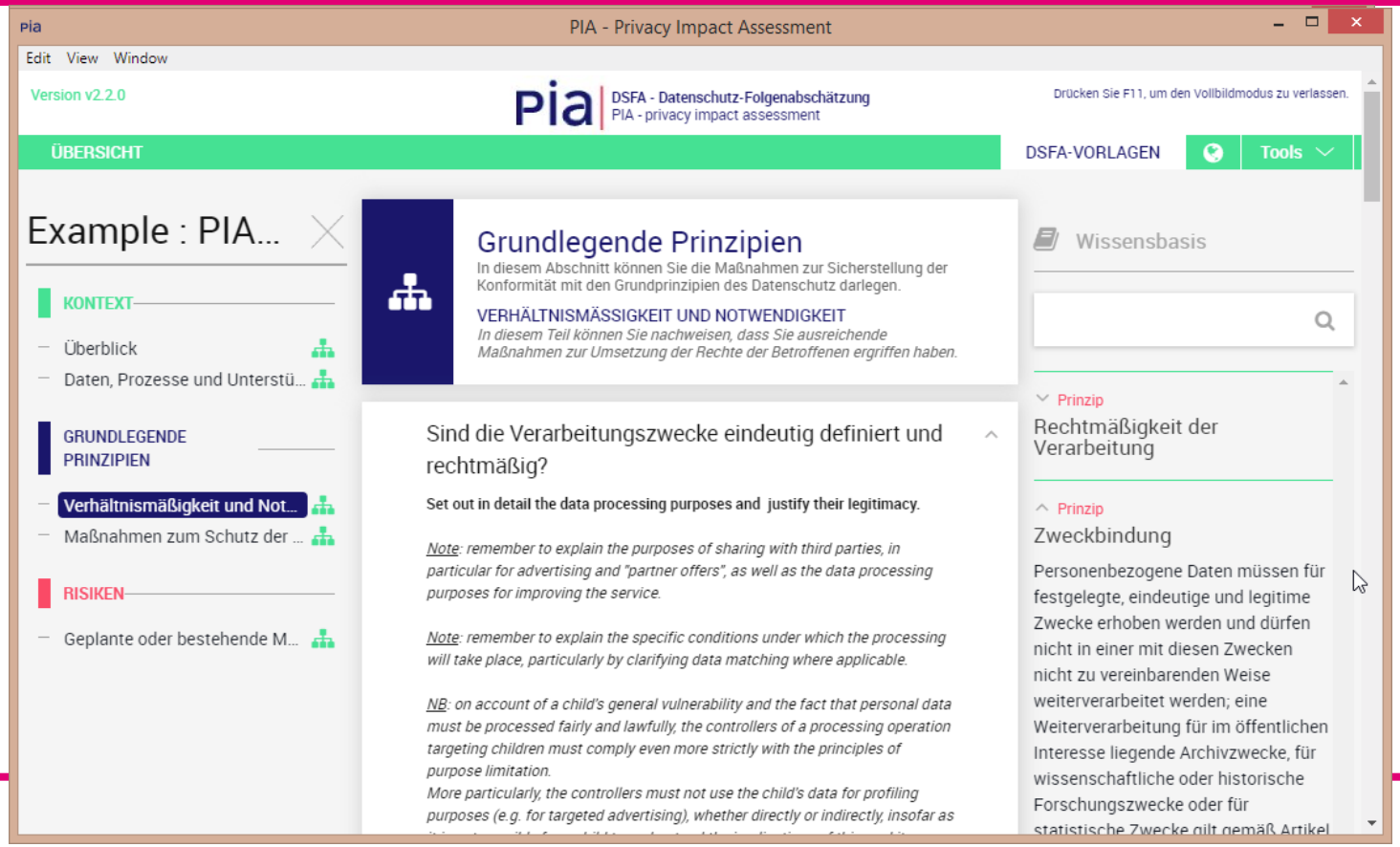
Beispiel bzgl. Umsetzung

Software der CNIL



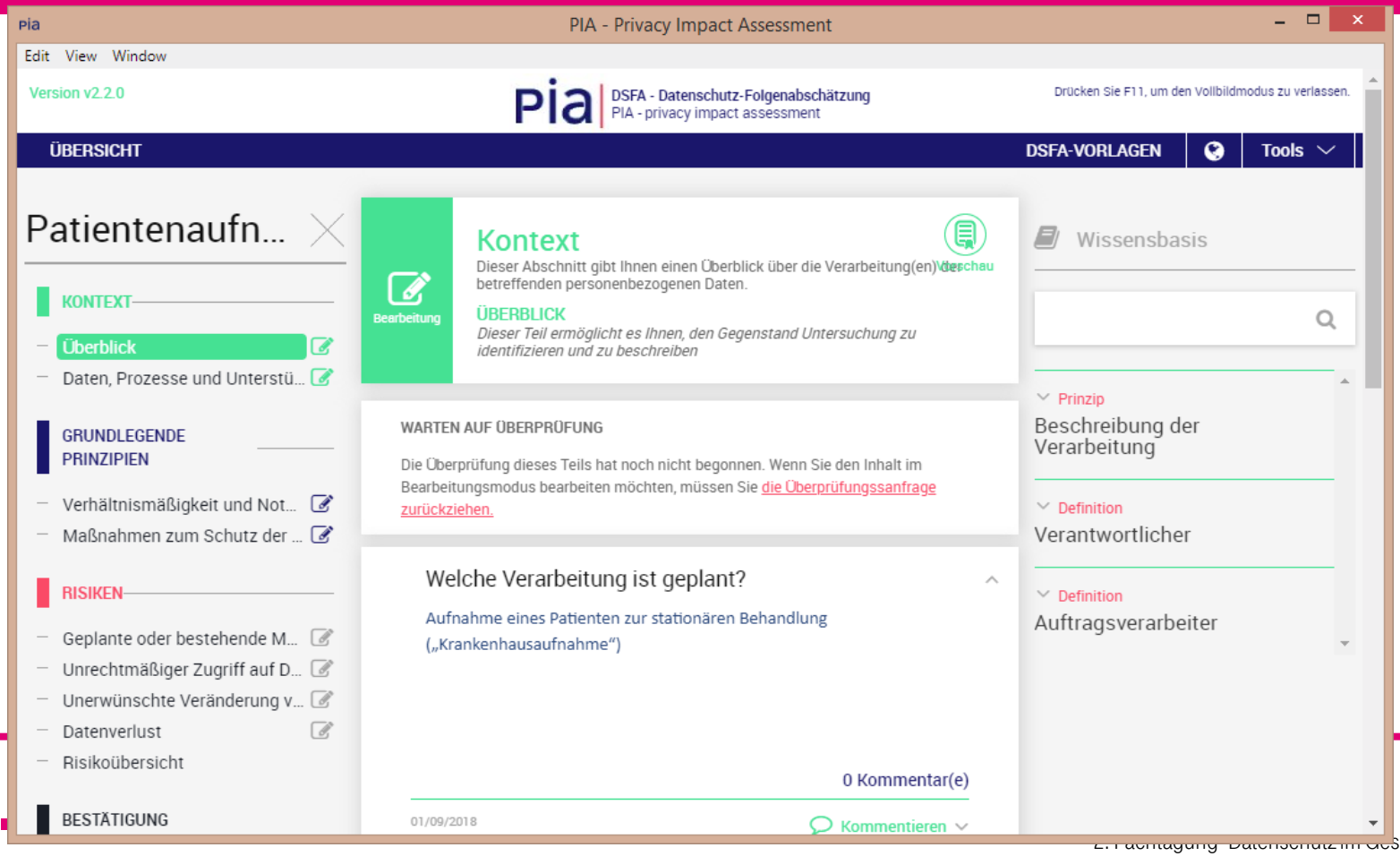
Beispiel bzgl. Umsetzung

Software der CNIL



Beispiel bzgl. Umsetzung

Software der CNIL



Beispiel bzgl. Umsetzung

Software der CNIL

Kurze Demo

Beispiel bzgl. Umsetzung

Software der CNIL: Anwendungshinweise

Gut:

- Software erlaubt Austausch von DSFA (Export als zip-json-File)
- DSFA-Report kann ausgedruckt und so Aufsichtsbehörde zur Verfügung gestellt werden

Aber:

- In einer DSFA müssen grundsätzlich alle erforderlichen Informationen in einem Detailgrad enthalten sein, dass ein Außenstehender – wie eine Aufsichtsbehörde – die DSFA lesen, nachvollziehen und bewerten kann
- Die Software verleitet dazu, Punkte nicht detailliert genug zu beschreiben, da sie dem Anwender viele Freiheiten lässt
- Daher: Die CNIL-Software kann man nur konform anwenden, wenn man auch die Erläuterungen in den pdf-Dateien beachtet
- Insbesondere Privacy Impact Assessment (PIA) 1 : methodology

Umsetzungshilfen: Ergebnisse AG bvitg, DKG, GMDS

Praxishilfe von bvitg, DKG, GMDS

Überarbeitete Version vom 17. September 2019

- Erste Praxishilfe wurde am 10. April 2018 veröffentlicht
- Umfangreiche und äußerst konstruktive Kommentierung der DSK bzw. des DSK-AK „Gesundheit und Soziales“
- Überarbeitete Version am 17. September 2019 veröffentlicht
  - Erläuterungen zum rechtlichen Hintergrund, d.h. Kommentierung Art. 35 (Kap. 3)
  - Darstellung von Vorgaben von Aufsichtsbehörden (Kap. 4)
  - Vorschlag zur Vorgehensweise bei einer DSFA (Kap. 5)
  - Vorschlag für die Strukturierung eines DSFA-Berichtes (Kap. 6)
  - Verschiedene Beispiele, z.B. für Datenarten, Verarbeitungszwecke (Kap. 7)
  - Literaturhinweise (Kap. 11)

Praxishilfe von bvitg, DKG, GMDS

Überarbeitete Version vom 17. September 2019

Datenschutz-Folgenabschätzung
gemäß Art. 35 DS-GVO

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.

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

Arbeitskreis „Datenschutz und IT-Sicherheit im Gesundheitswesen"

Deutsche Krankenhausgesellschaft e. V.

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.
Mark Rüdlin	Rechtsanwalt + Datenschutzbeauftragter
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Gerald Spyra	Ratajczak und Partner mbB Rechtsanwälte
Stefan Wunschel	Sana Kliniken AG

Version 2.0
Stand: 17. September 2019

Gemeinsame Praxishilfe von bvitg, DKG und GMDS

Stand: 2019-07-19

Download unter
https://gesundheitsdatenschutz.org/html/dsfa.php

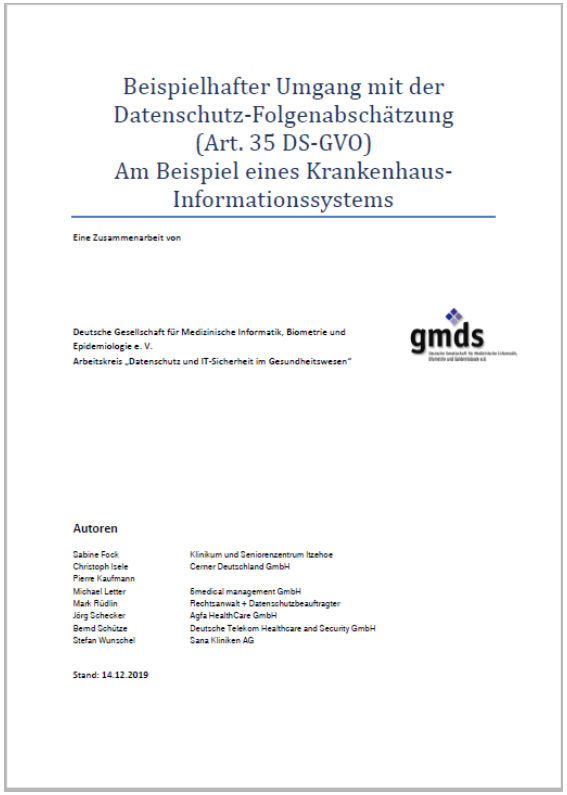
Beispiel DSFA von bvitg und GMDS

Beispiel DSFA für ein fiktives Krankenhaus-Informations-System (KIS)

- Basierend auf der Praxishilfe vom 2019-09-17 wurde beispielhaft eine DSFA für ein KIS erstellt
- Zweiteilig:
  1) Textuelle Beschreibung
     - des Verantwortlichen,
     - der Verarbeitungsvorgänge,
     - der Wahrung der Betroffenenrechte
     - ...
  2) Risikobetrachtung mit Tabellenkalkulation
     - Darstellung der Risiken, Risikoquellen
     - Risikoanalyse vor Maßnahmenbeginn
     - Risikoanalyse nach Maßnahmenfestlegung

Beispiel DSFA von bvitg und GMDS

Beispiel DSFA für ein fiktives Krankenhaus-Informations-System (KIS)



Beispielhafter Umgang mit der
Datenschutz-Folgenabschätzung
(Art. 35 DS-GVO)
Am Beispiel eines Krankenhaus-
Informationssystems

Eine Zusammenarbeit von

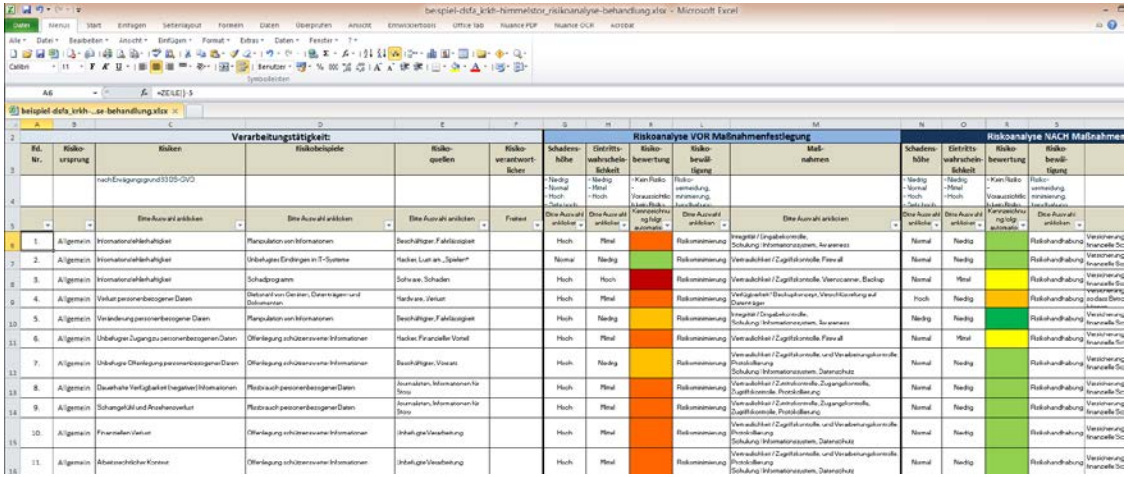
Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitskreis „Datenschutz und IT-Sicherheit im Gesundheitswesen"

gmds

Autoren

Sabine Fock	Klinikum und Seniorenzentrum Itzehoe
Christoph Isele	Cerner Deutschland GmbH
Pierre Kaufmann	
Michael Letter	6medical management GmbH
Mark Rüdlin	Rechtsanwalt + Datenschutzbeauftragter
Jörg Scheckler	Agfa HealthCare GmbH
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Stefan Wunschel	Sana Kliniken AG

Stand: 14.12.2019



Beispiel DSFA für KIS von bvitg und GMDS

Stand: 2019-12-14

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

Beispiel DSFA von bvitg und GMDS

Beispiel DSFA für ein fiktives Krankenhaus-Informations-System (KIS)

- Vorstellung des Beispiels

Diskussion / Fragen

Kontakt: Bernd.Schuetze@T-Systems.com