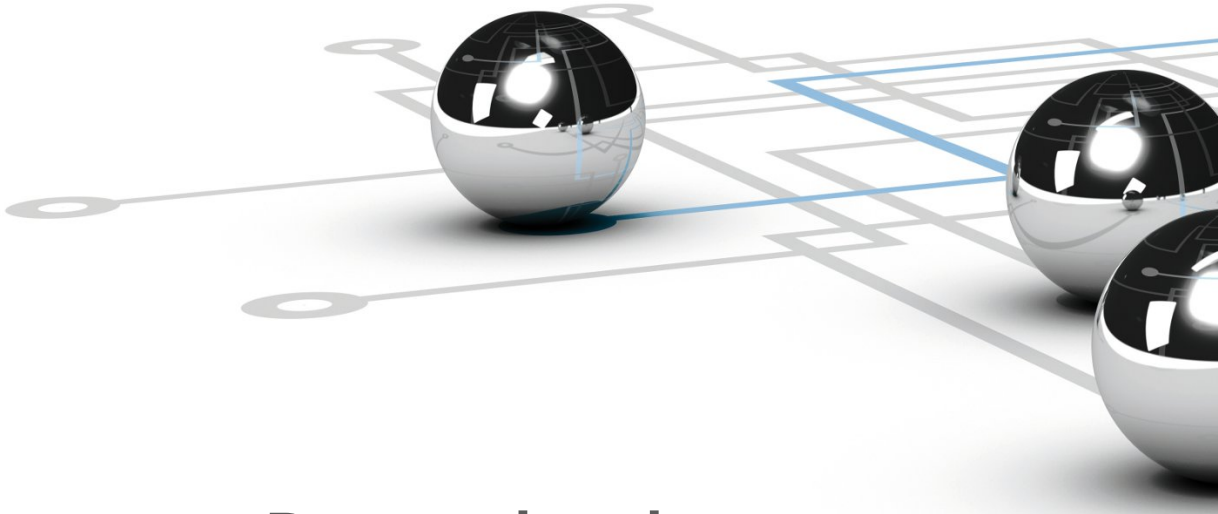
ZTG Zentrum für Telematik und Telemedizin GmbH



Stand der Ausarbeitung zum Datenschutzkonzept

GMDS Jahrestagung
01.09.2016, München

ZTG Zentrum für Telematik und Telemedizin GmbH
Dipl.-Inform. Med. Eric Wichterich, Dipl.-Soz.Wiss. Lars Treinat

Partner des GESUNDHEITSCAMPUS NORDRHEIN-WESTFALEN

Unser Profil

ZTG
Zentrum für Telematik und Telemedizin GmbH

bis 2012: Zentrum für Telematik im Gesundheitswesen

gefördert durch
Ministerium für Gesundheit, Emanzipation, Pflege und Alter des Landes Nordrhein-Westfalen

eGesundheit.nrw und die Telematik-Anforderungen

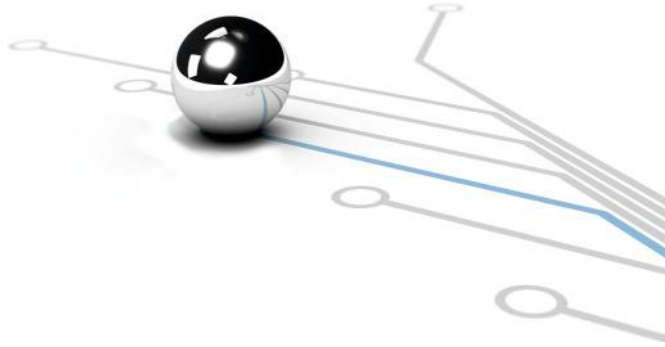
Förderdimensionen eG.nrw:

- Letzte Förderphase (IuK Gender & Altersgerechte Versorgungsmodelle): **25 Mio. €**
- Aktuelle Phase ab 2016 (Leitmarktwettbewerb): **20 Mio. €**

Ausganglage in der Praxis und Idee für Leitfaden

- **Ziel:** Schutz des Persönlichkeitsrechts der Betroffenen in den Projekten sichern
- **Methode:** Darstellung in einem Datenschutzkonzept
- **Problem:** Regelmäßig kein geeignetes Datenschutzkonzept vorhanden
- **Ursache:** Ungenügende Kenntnisse
  - …hinsichtlich Zweck eines DS-Konzeptes
  - …hinsichtlich Vorgehen bei Erstellung eines DS-Konzeptes
  - …hinsichtlich Aufbau/Struktur eines DS-Konzeptes
- **Lösung(?):** Leitfaden für Datenschutzkonzepte

Ziel des Leitfadens



- Niederschwelliger(er) Zugang für „Praktiker“
- Möglichst konkrete Ansage an Projektverantwortliche, zu welchen DS-Aspekten Aussagen benötigt werden
- Angemessenes Datenschutzniveau herstellen
- Gezielter Austausch und ggf. Vertiefung mit Datenschutz-Experten
- Prüfbarkeit der Projekte ermöglichen

Übersicht

Mustergliederung mit Hinweisen

„Standardisierung“ der Mustergliederung

Leitfaden ist seit Version 1.1 eine Zusammenarbeit von:

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

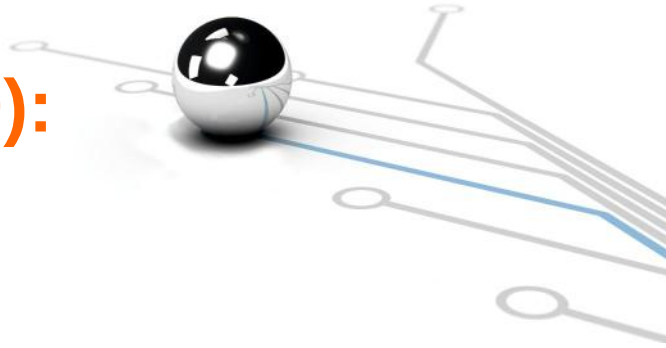
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Kontakt: **Dr. Bernd Schütze**

ZTG
Zentrum für Telematik und Telemedizin GmbH

Kontakt: **Eric Wichterich, Lars Treinat**

Lizenz des Leitfadens: Creative Commons (CC BY-SA 4.0):



Sie dürfen:

- Teilen
- Bearbeiten

Wenn:

- Namensnennung
- Weitergabe unter gleichen Bedingungen
- Keine weiteren Einschränkungen

https://creativecommons.org/licenses/by-sa/4.0/deed.de

VORGEHEN/AUFBAU DS-KONZEPT

Beschreibung des Vorhabens
(Fachliche Anforderungen)

→

Datenschutz-rechtliche Rahmen-bedingungen
(Materiell-rechtlicher Rahmen)

→

Datenschutz-bezogene Anforderungen
(Spezifische Datenschutz-anforderungen)

→

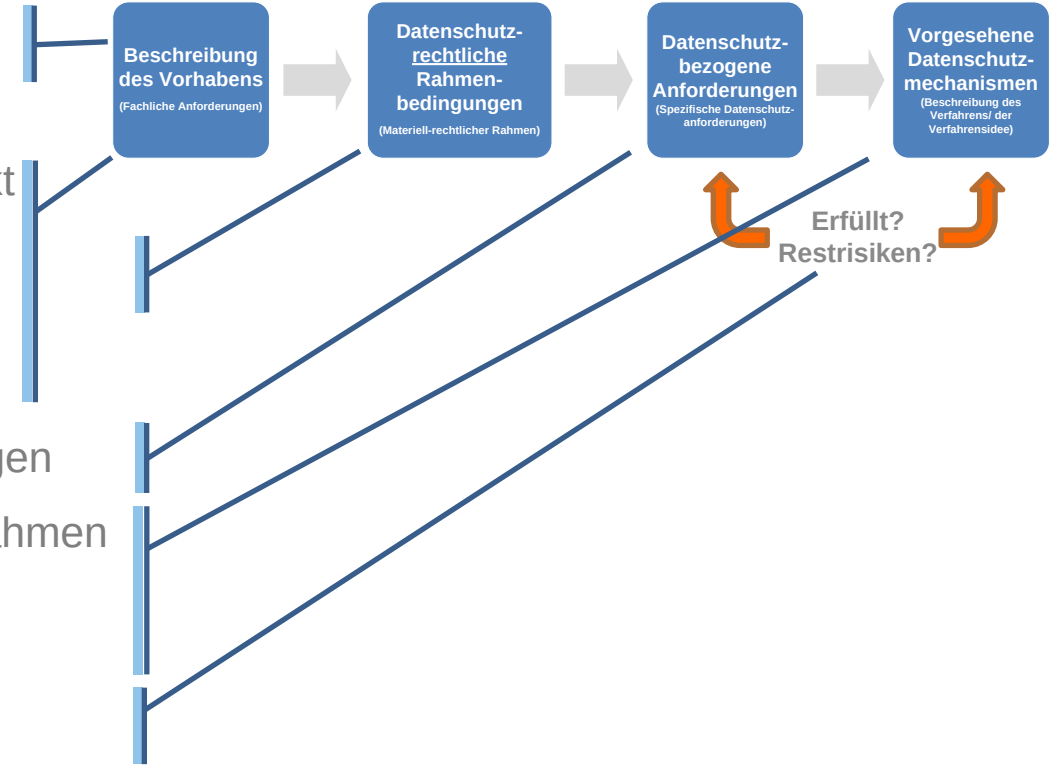
Vorgesehene Datenschutz-mechanismen
(Beschreibung des Verfahrens/ der Verfahrensidee)

Erfüllt?
Restrisiken?

(Vgl. auch: Elektronische Akten im Gesundheitswesen , S 30f.)
http://egesundheit.nrw.de/wp-content/uploads/2013/08/AKEPA-eFA.pdf

MUSTERGLIEDERUNG – ARBEITSSTAND V.1.1

1. Einleitung
2. Definitionen/Begrifflichkeiten
3. Fachliche Hintergründe zum Projekt
4. Beschreibung und Zielsetzung des Vorhabens
5. Akteure
6. Datenschutzbezogene Anforderungen
7. Implementierte Datenschutzmaßnahmen
8. Beschreibung der Umsetzung des Projektes/Skizzierung der Lösung
9. Konzeptuelle Risikobetrachtung
10. Mitgeltende Unterlagen



KAPITEL 1 „EINLEITUNG“

1. Einleitung
2. Definitionen/Begrifflichkeiten
3. Fachliche Hintergründe zum Projekt
4. Beschreibung und Zielsetzung des Vorhabens
5. Akteure
6. Datenschutzbezogene Anforderungen
7. Implementierte Datenschutzmaßnahmen
8. Beschreibung der Umsetzung des Projektes/Skizzierung der Lösung
9. Konzeptuelle Risikobetrachtung
10. Mitgeltende Unterlagen

Fragen/Hinweise

- Wie nenne ich das Vorhaben?
- Worum geht es (beschreiben Sie ganz kurz den Use Case/Anwendungsfall)?
- Wer führt das Projekt durch bzw. ist Ansprechpartner für Datenschutzkonzept?

Kapitel 2 „Definitionen/Begrifflichkeiten“

1. Einleitung
2. Definitionen/Begrifflichkeiten
3. Fachliche Hintergründe zum Projekt
4. Beschreibung und Zielsetzung des Vorhabens
5. Akteure
6. Datenschutzbezogene Anforderungen
7. Implementierte Datenschutzmaßnahmen
8. Beschreibung der Umsetzung des Projektes/Skizzierung der Lösung
9. Konzeptuelle Risikobetrachtung
10. Mitgeltende Unterlagen

Wichtig

- Leitfaden erhält ein Glossar: Bitte an definierte Begriffen halten, um einheitliches Verständnis zu wahren!
- Begriffe finden sich in der Regel in den Begriffsbestimmungen in den Gesetzen.
- Sollten Sie z. B. aufgrund von Begriffsbestimmungen in den von Ihnen anzuwendenden Gesetzen andere Definitionen als im Glossar des Leitfadens benutzen: Bitte in diesem Kapitel benennen!

KAPITEL 3 „FACHLICHE HINTERGRÜNDE ZUM PROJEKT“

1. Einleitung
2. Definitionen/Begrifflichkeiten
3. Fachliche Hintergründe zum Projekt
4. Beschreibung und Zielsetzung des Vorhabens
5. Akteure
6. Datenschutzbezogene Anforderungen
7. Implementierte Datenschutzmaßnahmen
8. Beschreibung der Umsetzung des Projektes/Skizzierung der Lösung
9. Konzeptuelle Risikobetrachtung
10. Mitgeltende Unterlagen

Fragen/Hinweise

Vgl. Lastenheft aus Kundensicht:

- Warum wird das Projekt durchgeführt?
- Welche Probleme sind die Motivation für das Projekt bzw. welche Probleme sollen gelöst werden?

KAPITEL 4 „BESCHREIBUNG UND ZIELSETZUNG DES VORHABENS“

1. Einleitung
2. Definitionen/Begrifflichkeiten
3. Fachliche Hintergründe zum Projekt
4. Beschreibung und Zielsetzung des Vorhabens
5. Akteure
6. Datenschutzbezogene Anforderungen
7. Implementierte Datenschutzmaßnahmen
8. Beschreibung der Umsetzung des Projektes/Skizzierung der Lösung
9. Konzeptuelle Risikobetrachtung
10. Mitgeltende Unterlagen

Fragen/Hinweise

1. Ziele

- Welche fachlichen Anforderungen sind bekannt?
- Sollen (und wenn ja welche) Geschäftsprozesse realisiert oder unterstützt werden?
- Was soll die Lösung bzw. das Projektergebnis können? usw.

2. Zweckbestimmung

- Wozu sind pers.bez. Daten erforderlich?

3. Verarbeitete Daten

- Welche Daten und welcher Schutzbedarf?

4. Rechtsgrundlage der DV

- Gesetzliche Befugnis? Einwilligungslösung?

5. Lebenszyklus der DV

- Von der Erhebung über die Nutzung bis hin zur Löschung.

Kapitel 5 „Akteure“

1. Einleitung
2. Definitionen/Begrifflichkeiten
3. Fachliche Hintergründe zum Projekt
4. Beschreibung und Zielsetzung des Vorhabens
5. Akteure
6. Datenschutzbezogene Anforderungen
7. Implementierte Datenschutzmaßnahmen
8. Beschreibung der Umsetzung des Projektes/Skizzierung der Lösung
9. Konzeptuelle Risikobetrachtung
10. Mitgeltende Unterlagen

Fragen/Hinweise

- Wer sind die Beteiligten und welche Rollen haben sie?
- In welcher rechtlichen Beziehung stehen die Beteiligten zu einander?
- Welche Weisungsbefugnisse gibt es?
- Wer sind die Projektverantwortlichen?
- Wer benutzt das Informationssystem?
- Wer führt Wartungsarbeiten durch oder greift aus anderen Gründen, die nicht der eigentlichen Nutzung entsprechen, auf das System zu?
- Werden Dienstleister eingesetzt?

KAPITEL 6 „DATENSCHUTZBEZOGENE ANFORDERUNGEN“

1. Einleitung
2. Definitionen/Begrifflichkeiten
3. Fachliche Hintergründe zum Projekt
4. Beschreibung und Zielsetzung des Vorhabens
5. Akteure
6. Datenschutzbezogene Anforderungen
7. Implementierte Datenschutzmaßnahmen
8. Beschreibung der Umsetzung des Projektes/Skizzierung der Lösung
9. Konzeptuelle Risikobetrachtung
10. Mitgeltende Unterlagen

Fragen/Hinweise

1. **Geeignetheit**
2. **Erforderlichkeit**
3. **Datenvermeidung/-sparsamkeit**
4. **Verhältnismäßigkeit/Übermaßverbot**
5. **Zweckbindung der DV, Aufbewahrungsfristen**
6. **Betroffenenrechte**
7. **Darstellung der Schutzziele**
   - Vertraulichkeit, Authentizität (Zurechenbarkeit), Integrität, Verfügbarkeit usw.
8. **Rechtskonformität**
   - Revisionsfähigkeit, Rechtssicherheit (eSig!), Nicht-Abstreitbarkeit

KAPITEL 7 „IMPLEMENTIERTE DATENSCHUTZMAßNAHMEN“

1. Einleitung
2. Definitionen/Begrifflichkeiten
3. Fachliche Hintergründe zum Projekt
4. Beschreibung und Zielsetzung des Vorhabens
5. Akteure
6. Datenschutzbezogene Anforderungen
7. Implementierte Datenschutzmaßnahmen
8. Beschreibung der Umsetzung des Projektes/Skizzierung der Lösung
9. Konzeptuelle Risikobetrachtung
10. Mitgeltende Unterlagen

Fragen/Hinweise

Vgl. Kapitel 6 – hier aber die Beschreibung der technisch-organisatorischen **Umsetzungen** der in Kap. 6 identifizierten Anforderungen

1. **Datenvermeidung/-sparsamkeit**
   - (etwa: Anonymisierung/Pseudonymisierung)
2. **Gewährleistung Betroffenenrechte**
3. **Maßnahmen zur Verteidigung der Schutzziele**

KAPITEL 8 „BESCHREIBUNG DER UMSETZUNG DES PROJEKTES/… “

1. Einleitung
2. Definitionen/Begrifflichkeiten
3. Fachliche Hintergründe zum Projekt
4. Beschreibung und Zielsetzung des Vorhabens
5. Akteure
6. Datenschutzbezogene Anforderungen
7. Implementierte Datenschutzmaßnahmen
8. Beschreibung der Umsetzung des Projektes/Skizzierung der Lösung
9. Konzeptuelle Risikobetrachtung
10. Mitgeltende Unterlagen

Fragen/Hinweise

- Bitte beschreiben bzw. skizzieren Sie Ihre ausgearbeitete Gesamtlösung.
- Der Leser soll einen Überblick über das konzipierte Verfahren erhalten.

Kapitel 9 „Konzeptuelle Risikobetrachtung“

1. Einleitung
2. Definitionen/Begrifflichkeiten
3. Fachliche Hintergründe zum Projekt
4. Beschreibung und Zielsetzung des Vorhabens
5. Akteure
6. Datenschutzbezogene Anforderungen
7. Implementierte Datenschutzmaßnahmen
8. Beschreibung der Umsetzung des Projektes/Skizzierung der Lösung
9. Konzeptuelle Risikobetrachtung
10. Mitgeltende Unterlagen

Fragen/Hinweise

- Cave: Es ist nicht zwingend die klassische „Risikoanalyse“ aus der IT-Sicherheitsanalyse gemeint.
- Anhand von in Kap. 8 beschriebene Lösung sollten denkbare Angriffsszenarien durchgespielt werden

  (Beispiel-Szenario: Unbefugte Person gibt sich für einen Patienten aus und verlangt die Löschung seiner Daten → z.B. Personalausweis-Kontrolle durchführen.)
- Bitte skizzieren Sie, wie groß/relevant das Risiko der identifizierten Angriffsszenarien ist und welche Maßnahmen die jeweiligen Angriffsszenarien abwehren würden?

Kapitel 10 „Mitgeltende Unterlagen“

1. Einleitung
2. Definitionen/Begrifflichkeiten
3. Fachliche Hintergründe zum Projekt
4. Beschreibung und Zielsetzung des Vorhabens
5. Akteure
6. Datenschutzbezogene Anforderungen
7. Implementierte Datenschutzmaßnahmen
8. Beschreibung der Umsetzung des Projektes/Skizzierung der Lösung
9. Konzeptuelle Risikobetrachtung
10. Mitgeltende Unterlagen

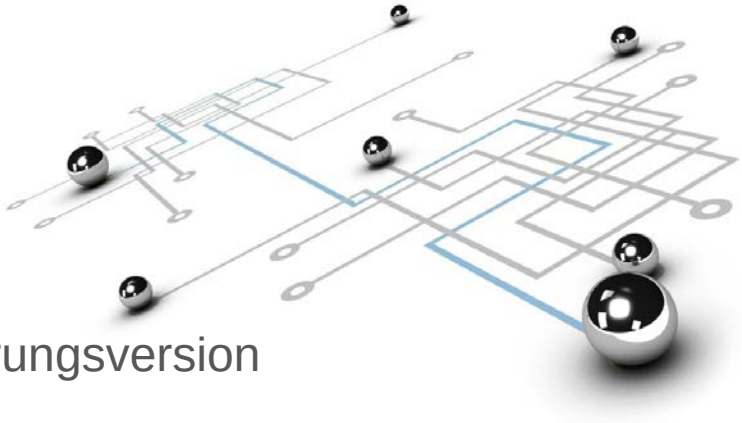
Fragen/Hinweise

- Ergänzende Unterlagen, die für das DS-Konzept relevant sind, z. B.
  - Berechtigungskonzept (Rollen- und Rechtekonzept)
  - Datenschutzrichtlinie
  - Verfahrensverzeichnis der Verantwortlichen Stelle bzw. Verzeichnis von Verarbeitungstätigkeiten
  - Protokollierungskonzept
  - Löschkonzept
  - Sicherheitskonzept
  - Notfall-Handbuch
  - Archivordnung
  - Musterdokumente wie: Patienteninformation, Patientenaufklärung, Patienteneinwilligung, Schweigepflichtentbindung, usw.

Laufende Arbeiten

- Weiterentwicklung des Leitfadens gemeinsam mit der GMDS-AG DIG, **Publikation v.1.1 voraussichtlich Dezember 2016**
- Abstimmung mit Aufsichtsbehörden (aktuell LDI NRW)
- Vorstellung in Fachkreisen und Aufnehmen von Feedback
- Vorbereitungen für einen ERFA-Kreis für Zuwendungsempfänger und kleine Einrichtungen

ZEITPLAN



- 17. Oktober: Finalisierung einer Kommentierungsversion

- 18.10 -11.11: Kommentierungsphase
- 12.-25.11: Überarbeitungsphase, Auflösung Kommentierungen
- 09.12.: Abschlussbesprechung und Finalisierung
- 12.12.: Veröffentlichung

Fragen?

Wir sind für Sie da!

Dipl.-Inform. Med.
Eric Wichterich
e.wichterich@ztg-nrw.de

Dipl.-Soz.Wiss.
Lars Treinat
l.treinat@ztg-nrw.de

ZTG Zentrum für Telematik und Telemedizin GmbH
Universitätsstraße 142
44799 Bochum
Geschäftsführer: Rainer Beckers, M.P.H., M.A.; Lars Treinat, Dipl.-Soz.Wiss.

Abb. © Sebastian Kaulitzki - Fotolia