



Leitfaden für die Erstellung von Datenschutzkonzepten

GMDS Jahrestagung 30.08.2016, München

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



UNSER PROFIL



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

@Gesundheit.nrw

Ministerium für Gesundheit, Emanzipation, Pflege und Alter des Landes Nordrhein-Westfale





Anforderungen für Förderprojekte aus dem Bereich "Telematik & Telemedizin"

Die Zuwendungsempfängerinnen und Zuwendungsempfänger verpflichten sich, im Rahmen der Projektdurchführung folgende <u>Anforderungen der Landesinitiative eGesundheit.nrw</u> zu berücksichtigen:

- Nutzen- und Nutzerorientierung
 - Gebrauchstauglichkeit von Hardware- und Softwarekomponenten durch die Einbindung von Nutzerinnen und Nutzern.
 - Sicherstellung des Nutzens: nutzenbasierte Spezifikation von Lösungsbausteinen und Evaluation des Nutzens der Projektergebnisse.
 - Datenschutz und IT-Sicherheit: Einhaltung der gesetzlichen Datenschutzbestimmungen (Persönlichksirzecht und informationelle Selbstestimmung der Bertoffenen) und Sicherstellung der Wahrung der ärztlichen Schweigepflicht. Darstellung in einem Datenschutzkonzept und Informationsicherheitskonzent. Weiterhin die Berticksichtigung und Ntutzun gertügbarer Authentifikationsmittel, wie der elektronischen Gesundheitskarte und elektronischer Heilberufsausweise.
- Wiederverwendbarkeit und Nachhaltigkeit
 - Infrastruktur und Datenübermittlung: Berücksichtigung und Nutzung verfügbarer und projektspezifisch sinnvoll nutzbarer Infrastrukturkomponenten und Dienste aus dem Projekt zum Aufbau einer nationalen Telematiisinfrastruktur für das Gesundheitswesen und der im Land NRW vorhandenen Infrastrukturkomponenten bzw. Infrastruktur.
 Sicherer technischer Austauch von Daten und elektronischen Dokumenten auf Basis anerkannter
 - Sicherer technischer Austausch von Daten und elektronischen Dokumenten auf Basis anerkannter Standards und Lösungen, wie der elektronischen Fallakte, KV-Connect oder KV-SafeNet.
 - Nationale Anwendungen: Berücksichtigung und Nutzung von im Rahmen des Aufbaus der nationalen Telematikinfrastruktur erarbeiteten fachlogischen Lastenhefte, Spezifikationen, Datenmodelle, Verfahrensbeschreibungen, z. B. Bundesmedikationsplan, Notfalldatensatz.
 - Weiternutzung von Ergebnissen anderer Projekte: Berücksichtigung der Ergebnisse aus themennahen Projekten der Landesinitiative eGesundheit.nrw.
 - Interoperabilität und Interoperabilitätsspezifikationen: Spezifikationen müssen transparent, diskriminierungsfrei und an internationalen Standards orientiert in Form von Leitfäden erstellt werden. Für Behandlungsdokumente sind diese auf CDA aufzubauen und als CDA-Leitfäden zur Verfügung zu stellen.
- Transparenz und Synergie
 - Projektrepository: Das Projekt sowie der Projektfortschritt sind im eGesundheit.nnw-Projektrepository (Wiki) entsprechend dem dort vorgegebenen Raster einzupflegen und regelmäßig (mindestens alle 3 Monate) fortzuschreiben.
 - SDIS Standards-Dokumentations- und Informationssystem: Die im Rahmen der Projektarbeit gefundenen und nicht in SDIS enthaltenen Standards sind dort einzupflegen und die Nutzung von Standards im Projekt entsprechend zu doku- mentieren. Dies triffte benso auf die im Projekt auf Basis bestehender Standards angepassten oder neu entwickelten Interoperabilitätsspezifikationen zu.
 - Semantik: Berücksichtigung und Nutzung von im Terminologieserver enthaltenen Semantikfestlegungen oder international vorhandener Ordnungssysteme.
 Die im Rahmen der Projektarbeit gefundenen und nicht im Terminologieserver enthaltenen oder angepassten/neu definierten Semantikfestlegungen sind dort einzupflegen.

Träger der Landesinitiative und Ansprechpartner für alle Fragen zu eGesundheit.nrw ist die ZTG Zentrum für Telematik und Telemedizin GmbH in Bochum.



Telematik-Anforderungen für geförderte Projekte in NRW

- 1. Nutzen- und Nutzerorientierung
- Wiederverwendbarkeit und Nachhaltigkeit
- 3. Transparenz und Synergie
- → http://wiki.egesundheit.nrw.de

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:



Arbeitsgruppe "Datenschutz und IT-Sicherheit im Gesundheitswesen"

Kontakt: Dr. Bernd Schütze



Kontakt: Eric Wichterich, Lars Treinat

LIZENZ DES LEITFADENS: CREATIVE COMMONS – BY – SA:



Sie dürfen:

- Teilen
- Bearbeiten

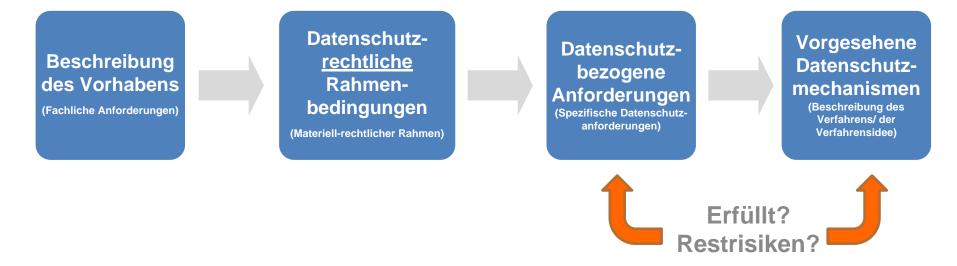
Wenn:

- Namensnennung
- Weitergabe unter gleichen Bedingungen
- Keine weiteren Einschränkungen



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

VORGEHEN/AUFBAU DS-KONZEPT

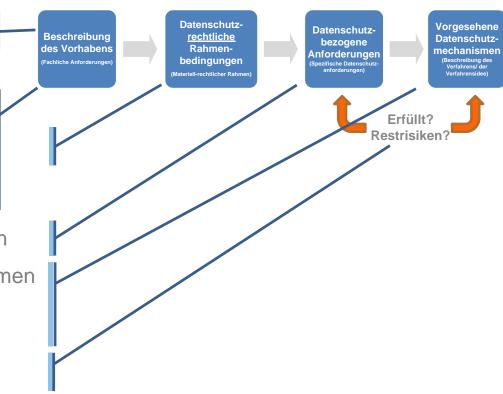




(Vgl. auch: Elektronische Akten im Gesundheitswesen, S 30f.) http://egesundheit.nrw.de/wp-content/uploads/2013/08/AKEPA-eFA.pdf

MUSTERGLIEDERUNG - ARBEITSSTAND V.1.1

- 1. Einleitung
- 2. Definitionen/Begrifflichkeiten
- 3. Fachliche Hintergründe zum Projekt
- 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 2 "DEFINITIONEN/BEGRIFFLICHKEITEN"

- 1. Einleitung
- 2. Definitionen/Begrifflichkeiten
- 3. Fachliche Hintergründe zum Projekt
- 4. Beschreibung und Zielsetzung des Vorhabens
- 5. Akteure
- 6. Datenschutzbezogene Anforderungen
- Implementierte Datenschutzmaßnahmen
- 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 1 "EINLEITUNG"

1. Einleitung

- 2. Definitionen/Begrifflichkeiten
- 3. Fachliche Hintergründe zum Projekt
- 4. Beschreibung und Zielsetzung des Vorhabens
- Akteure
- 6. Datenschutzbezogene Anforderungen
- 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 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
- 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
- Akteure
- 6. Datenschutzbezogene Anforderungen
- 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
- 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
- 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
- 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
- Akteure
- 6. Datenschutzbezogene Anforderungen
- 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
- Implementierte Datenschutzmaßnahmen
- 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?

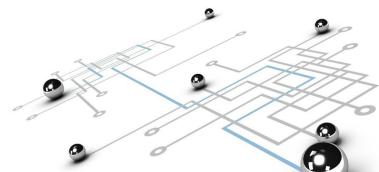
KAPITEL 10 "MITGELTENDE UNTERLAGEN"

- 1. Einleitung
- 2. Definitionen/Begrifflichkeiten
- 3. Fachliche Hintergründe zum Projekt
- 4. Beschreibung und Zielsetzung des Vorhabens
- Akteure
- 6. Datenschutzbezogene Anforderungen
- Implementierte Datenschutzmaßnahmen
- 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

Anregungen?

<u>Ihr</u> Input ist uns herzlich willkommen!



Fragen?

Wir sind für Sie da!

Dipl.-Inform. Med.

Eric Wichterich

e.wichterich@ztg-nrw.de

Dipl.-Soz.Wiss.

Lars Treinat

I.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.





2ZTG GmbH