Cybersecurity und Datenschutz im Gesundheitsbereich Konflikte und Synergien

Session 5

Big Data in Health Care

Workshop on Ethics and Cybersecurity in Health Care
Fachtagung im Rahmen des EU-geförderten Projekts CANVAS
Regensburg, 25.04.2018

Eva Schlehahn, Harald Zwingelberg, Martin Rost, Felix Bieker
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Was soll durch Datenschutz geschützt werden?

- Datenschutzrecht schützt natürliche Personen!

- Warum?
  - Datenschutz gleicht Machtasymetrien zwischen Personen und (datenverarbeitenden) Organisationen aus.

Verhältnis IT Sicherheit und Datenschutz

- **IT Sicherheit unterstellt methodisch: Jede Person kann ein Angreifer sein!**

- **Datenschutz unterstellt: Jede Organisation ist ein Angreifer!**

➢ Daher:
  - Organisationen müssen Personen nachweisen dass sie keine Angreifer sondern vertrauenswürdig sind.
  - Dies kann u. a. dadurch gelingen, indem Organisationen sich bei personenbezogenen Verfahren nachweisbar an Gesetze und transparente Regeln halten

  - Für Kryptologen: Insbesondere **Bob ist der Angreifer**!

Perspektive und Zielvorstellung des Datenschutzes

- **Grundrechtsschutz!**
- Aber was sind Grundrechte eigentlich?
  - Abwehrrechte Bürger gegen den Staat
  - Mittelbare Drittwirkung gegen Private
  - Begründen Schutzpflichten des Staates
    - Selbstbindung bei staatlichem Handeln und
    - Effektiver Grundrechtsschutz durch Organisation und Verfahren

- Insoweit Grundrechtseingriffe **nur unter besonderen Voraussetzungen** und **mit Rechtfertigung**

Grundlegendes zum Verständnis des Datenschutzes

- Verbot mit Erlaubnisvorbehalt

➢ Es braucht IMMER eine Rechtsgrundlage!

  - Besonderer Geheimnisschutz im Gesundheitssektor (ärztliche Schweigepflicht)
  - Daher dürfen Daten dürfen nur dann erhoben, verarbeitet und übermittelt werden, wenn **bereichsspezifische** Regelungen dies erlauben.
  - Gesetzesgrundlagen für Datenerhebung:
    - Allgemein Art. 6 DSGVO
    - Für Gesundheitsbereich Art. 9 DSGVO, Sozialrecht SGB X

- Dazu: Grundsätze des Art. 5 DSGVO (s. Folgefolie)

Ganz allgemein: Grundsätze Art. 5 DSGVO

- Rechtmäßigkeit der Verarbeitung
- Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung (Erforderlichkeit)
- Richtigkeit der Datenverarbeitung
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Details zu Grundprinzipien Art. 5 DSGVO

- **Zweckbindung:** Zweck von Erhebung und Verarbeitung muss **hinreichend bestimmt** sein.
  - Rahmen ist in der Regel das konkrete Behandlungsverhältnis

- **Erforderlichkeit:** Umfang von Erhebung und Verarbeitung der Daten muss erforderlich sein.

➢ **Big Data relevant:**

- Spezielle Regelungen z.B. für Forschung, Archive, Statistik beachten: Artikel 9 (2) (j) DSGVO i. V. m. nationalen Gesetzen wie § 27 BDSG-neu, §§ 13, ggf. Landesdatenschutzgesetze (wie etwa 26 LDSG-SH-Entwurf 2018)

Der Begriff „Risiko" im Datenschutz

Ein Grundrechts-Eingriff ist liegt schon bei einer Durchführung eines personenbezogenen Verfahren vor!

- Das gilt auch dann wenn diese
  - durch eine Rechtsgrundlage gerechtfertigt ist und
  - nachgewiesen sichere IT eingesetzt wird.
- Insofern liegt da schon ein „**eingetretenes Risiko**" vor.

➢ Der Eingriff muss dann durch technische und organisatorische Schutzmaßnahmen auf das unbedingt erforderliche Maß verringert werden.

- Eingriff erzeugt Risiken und unmittelbare (physische, materielle, immaterielle) Folgen für die einzelnen Betroffenen
- Mittelbare Folgen für alle Personen aufgrund gesellschaftlicher Strukturschädigungen

Definition Risiko

- Risiko im Sinne der DSGVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.
- Es hat zwei Dimensionen:
  1. die Schwere des Schadens und
  2. die Wahrscheinlichkeit,

  dass das Ereignis und die Folgeschäden eintreten.

7 typische Risiken im Datenschutz

Risiko 1	Risiko 2	Risiko 3	Risiko 4	Risiko 5	Risiko 6	Risiko 7
Eine Organisation betreibt ein **nicht legitimes personenbe-zogenes Verfahren.**	Die **Schwere des Grundrechtseingriffs** durch ein legitimes pbV wird nicht oder falsch bestimmt, Rechtsgrundlage reicht nicht oder wurde unzureichend geprüft, Die Verantwortungsüber-nahme ist unklar.	Eine Organisation betreibt ein im Grundsatz ordnungsgemäßes pbV, **dehnt oder ändert jedoch den Zweck** (Vorratsdatenspeic herung, Big Data).	Eine Organisation betreibt für ein pbV **keine hinreichend wirksamen Maßnahmen der IT-Sicherheit.**	Eine Organisation betreibt für ein pbV die Maßnahmen der **IT-Sicherheit nicht grundrechts-konform**.	Das **Angreifermodell** bzgl. anderer (befugt) zugreifender Organisationen (z.B. Sicherheitsbehör den) ist **falsch oder unterkomplex** angelegt.	Die pbV von Organisatio nen werden **nicht ausreichend geprüft und beurteilt.**

Risiko 1 : Legitimität eines Verfahrens ist ungeklärt

- Illegitime Verfahren lassen sich **nicht nachträglich** durch Gesetz, Einwilligungen oder durch das Installieren von Schutzmaßnahmen legitimieren/legalisieren!

Verantwortliche, Datenschutzaufsichtsbehörden und Gerichte müssen die Legitimität von Verfahren(stypen) kontrollieren, prüfen und beurteilen.

Art. 35 DSGVO **Datenschutz-Folgenabschätzung** kann Schutz vor nicht-legitimen Verfahren entfalten, weil konsistenter als bislang jedes Verfahren zu prüfen ist.

- Eintrittswahrscheinlichkeit? Hoch

Durch bspw. Facebook, Google / Apple findet Vollüberwachung von Personen statt; inzw. ist eine kulturelle Gewöhnung an eine Vollüberwachung der menschlichen „Laborratten" (Wehler) und „Zombies" (Kutscha) eingetreten, too big to fail.

- Schwere des Risikos? Hoch

Illegitime Verfahren unterlaufen soziale Schutzvorkehrungen moderner Gesellschaften, sie führen zur **De-legitimierung des Rechts und der Institutionen**, Auslieferung von Personen an Privatorganisationen findet statt, staatliche Exekutive bedient sich zudem der Infrastrukturen und Datenbestände der Kommunikations-unternehmen zur Vollüberwachung der Bürger.

Risiko 2 : Falsche Bestimmung Schwere des Grundrechtseingriffs

- Empfehlenswert: **Typisierung der Grundrechtseingriffe, um die Schwere einzuordnen** (z.B. „leicht, mittel, schwer" nach der Alexy-Formel*). Bislang jedoch keine Praxis in der Datenschutzaufsicht.

Nicht Sensitivität personenbezogener Daten, sondern Eingriffsintensität ist maßgeblich.

Es bedarf eines umfassenden spezifischen Angreifermodells des Datenschutzes in Abgrenzung zum Angreifermodell der IT-Sicherheit.

Falsche Bestimmung der Schwere eines Grundrechteeingriffs führt zu einer falschen Bestimmung der Wirksamkeit von zu treffenden Schutzmaßnahmen, die die Eingriffsintensität auf das geringstmögliche Maß mildern könnten.

- Eintrittswahrscheinlichkeit? Hoch

Weil keine Übung in der juristischen Entscheidungsfindung, und wenn ausnahmsweise doch genutzt dann ist es folgenlos für Bestimmung der Maßnahmen.

- Schwere des Risikos? Hoch

Beeinträchtigt Personen unmittelbar. Eine unangemessen leichte beliebige Verkettbarkeit von Daten unterläuft strukturelle Schutzvorkehrungen moderner Gesellschaften mit der Folge der Zerstörung von Strukturen und Auslieferung von Personen an rechtlich nicht eingefangene Organisationen.

* Alexy, Robert, 2003: Die Gewichtsformel, in: Jickeli, J.; Kreutz, P.; Reuter, D., 2003: Gedächtnisschrift für Jürgen Sonnenschein, Berlin, De Gruyter Verlag, S. 777ff.

Risiko 3: Zweckküberdehnung bei der Anwendung eines Verfahrens

- Die **Zwecksetzung** muss legitim sein, die **Zweckbestimmung** muss hinreichend eng und prüfbar erfolgen, die **Zwecktrennung** und die **Zweckbindung** erleichtern die operative Umsetzung und die Prüfbarkeit eines Verfahrens.

Die Zweckbestimmung bildet den **definitorischen Kern eines pb Verfahrens**, aus dem heraus die erforderlichen Daten, IT-Systeme und Prozesse sowie die Schutzmaßnahmen zu bestimmen sind.

Zweckdehnung findet durch **häufig übermäßige Ausnutzung der Einwilligung** statt, die als vermeintlich souveräner Akt gesehen wird.

Zweckdehnung/-entfremdung sind in der Praxis von Big Data zum Alltag geworden.

Abhilfe z. B. durch breite Nutzung von anyonymen Transaktions-Credentials in Kommunikations-beziehungen möglich.

- Eintrittswahrscheinlichkeit? Hoch

Eine Organisation, die nicht den maximal möglichen Informationsschatz hebt, gerät im Benchmark mit anderen Organisationen ins Hintertreffen, zumal keine gleichmäßig gestreuten, sondern nur „ungerecht punktuelle" Datenschutzprüfungen erfolgen (dadurch „Marktverzerrung").

- Schwere des Risikos? hoch

Beeinträchtigt Personen unmittelbar. Kein fairer Tausch. Eine Ausweitung der Zweckbestimmungen unterläuft ebenfalls strukturelle Schutzvor-kehrungen moderner Gesellschaften mit der Folge der Auslieferung von Personen an Organisationen.

Risiko 4
Mangelhafte IT-Sicherheitsmaßnahmen

- Die IT- bzw. Informationssicherheit bspw. nach **IT-Grundschutz schützt nur die Assets einer Organisation. Die Organisation sieht sich aber oft nicht selbst als Angreiferin!**

Erwägungsgrund 75 DSGVO:

- Diskriminierung,
- Identitätsdiebstahl oder -betrug,
- Finanzieller Verlust,
- Rufschädigung,
- Wirtschaftliche oder gesellschaftliche Nachteile,
- Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen.

- Eintrittswahrscheinlichkeit? Hoch

Die Leitungen von Organisationen wissen inzwischen, dass sie ihre IT mit Schutzmaßnahmen ausstatten müssen. These: Gute IT-Sicherheit = guter Datenschutz ist falsch. Und: **Es gibt keine sichere IT.**

- Schwere des Risikos? Hoch

Ein unbefugter Zugriff auf ein Verfahren (auf Daten, IT-Systeme und Prozesse) führt zu einer beliebigen Datenverarbeitung mit teilweise konkreten **materiellen und immateriellen Schäden und unabsehbaren Folgen** für Betroffene und für Gesellschaft (bspw. Wahlbeeinflussung)

Risiko 5: Mangelhafter Datenschutz bei IT-Sicherheitsmaßnahmen

Das **IT-Sicherheitsmanagement ist etabliert** und hat in den letzten 10 Jahren drastisch an Qualität gewonnen.

Methodisch sind IT-SiBe ungleich besser ausgebildet und ausgerüstet als Datenschutzbeauftragte, sie haben in den Organisationen gestalterisch gleich nach dem CIO den Lead.

- Rechtsdogmatisch muss Datenschutz die IT-Sicherheit führen, in der Praxis läuft es genau umgekehrt.

Ganz schlechte Datenschutz-Awareness bei Administratoren bzw. „IT'lern", diese setzen erfahrungsgemäß Maßnahmen der IT-Sicherheit mit denen des operativen Datenschutz gleich, im Konfliktfall zu Lasten der Betroffenen.

- Eintrittswahrscheinlichkeit? Hoch

IT'ler agieren im Auftrag der Organisationsleitung und verstehen den Unterschied zw. IT-Sicherheit für personenbezogene Daten und operativem Datenschutz als Grundrechteschutz meist nicht.

- Schwere des Risikos? Hoch

Schutzmaßnahmen der IT-Sicherheit im Interesse der Organisation dominieren in der Praxis operative Maßnahmen des Datenschutzes.

Risiko 6
Falsches oder schwaches Angreifermodell

- Der **Hauptangreifer ist immer die datenverarbeitende Organisation** selbst.

Darüber hinaus gibt es **weitere typische Angreifer-Organisationen** auf Personen:

- Sicherheitsbehörden
- Leistungsverwaltung
- Bereitsteller von IT-(Infrastruktur)Diensten
- Bereitsteller kritischer Infrastrukturen (wie Energieversorger)
- Versicherungen und Banken
- Forschungsinstitute
- Krankenhäuser, Ärzte, Dienstleister
- Untätige Aufsichtsbehörden
- Hacker
- ...

- Eintrittswahrscheinlichkeit? Hoch

Es besteht, im Unterschied zur IT-Sicherheit, keine Übung, auch für Datenschutz ein spezifisches Angreifermodell zu formulieren. Ist eine Provokation, „sich selbst" als primäre Konfliktquelle anzusetzen.

- Schwere des Risikos? Hoch

Ein befugter Zugriff auf ein Verfahren (auf Daten, IT-Systeme und Prozesse), auf den der Betroffene keinen Einfluss hat, kann zu einer beliebigen Datenverarbeitung mit teilweise konkreten **materiellen und immateriellen Schäden und unabsehbaren Folgen** für Betroffene und für Gesellschaft führen.

Risiko 7: Mangelhafte Datenschutzkontrolle: Institutionenversagen

Verschiedene Fallkonstellationen möglich:

- Personenbezogene Verfahren werden nicht durch unabhängige Datenschutzaufsichtsbehörden geprüft; oder
- pb Verfahren werden zwar geprüft aber die Prüfungen sind unsystematisch oder setzen methodisch falsch an oder sind unvollständig oder nicht intensiv (Prüfintegrität); oder
- Prüfungen werden zwar integer durchgeführt, aber negative Prüfergebnisse seitens der Datenschutzaufsicht bleiben ohne nachhaltige Konsequenzen für den verantwortlichen Datenverarbeiter; oder
- die Datenschutzaufsicht bringt zwar Konflikte vor Gericht, aber das Gericht entscheidet nicht in der Sache; oder
- das Gericht entscheidet zwar in der Sache, aber die gesetzliche Regelung ist unzureichend.

➢ Eintrittswahrscheinlichkeit? Hoch

Die Zahl integrer externer Datenschutzprüfungen, methodisch integrer Prüfungen sowie datenschutz-relevanter Gerichtsentscheidung ist gemessen an der Zahl der Verstöße verschwindend gering.

➢ Schwere des Risikos? Hoch

Willkürlich erfolgende Sanktionen de-legitimieren das Rechts- und Politiksystem und zerstören dadurch wesentliche gesellschaftliche Schutzstrukturen zur Pazifizierung von Organisationen gegenüber Personen.

Fortentwicklung des Datenschutzes durch Bearbeitung der aufgeführten Risiken

Zur Erinnerung:

- Zielvorstellung aus Datenschutz-Sicht ist:
  - Eingriff muss durch technisch-organisatorische Schutzmaßnahmen auf das unbedingt erforderliche Maß verringert werden.

- Frage ist: Wo spielt Cybersecurity mit rein?

Risikobeurteilung

1. Risikoidentifikation
   - Welche Schäden können entstehen?
   - Durch welche Ereignisse können Schäden entstehen?
   - Durch welche Handlungen/Umstände können Ereignisse eintreten?
2. Abschätzung von
   - Eintrittswahrscheinlichkeit
   - Schwere möglicher Schäden
3. Zuordnung zu Risikoabstufungen

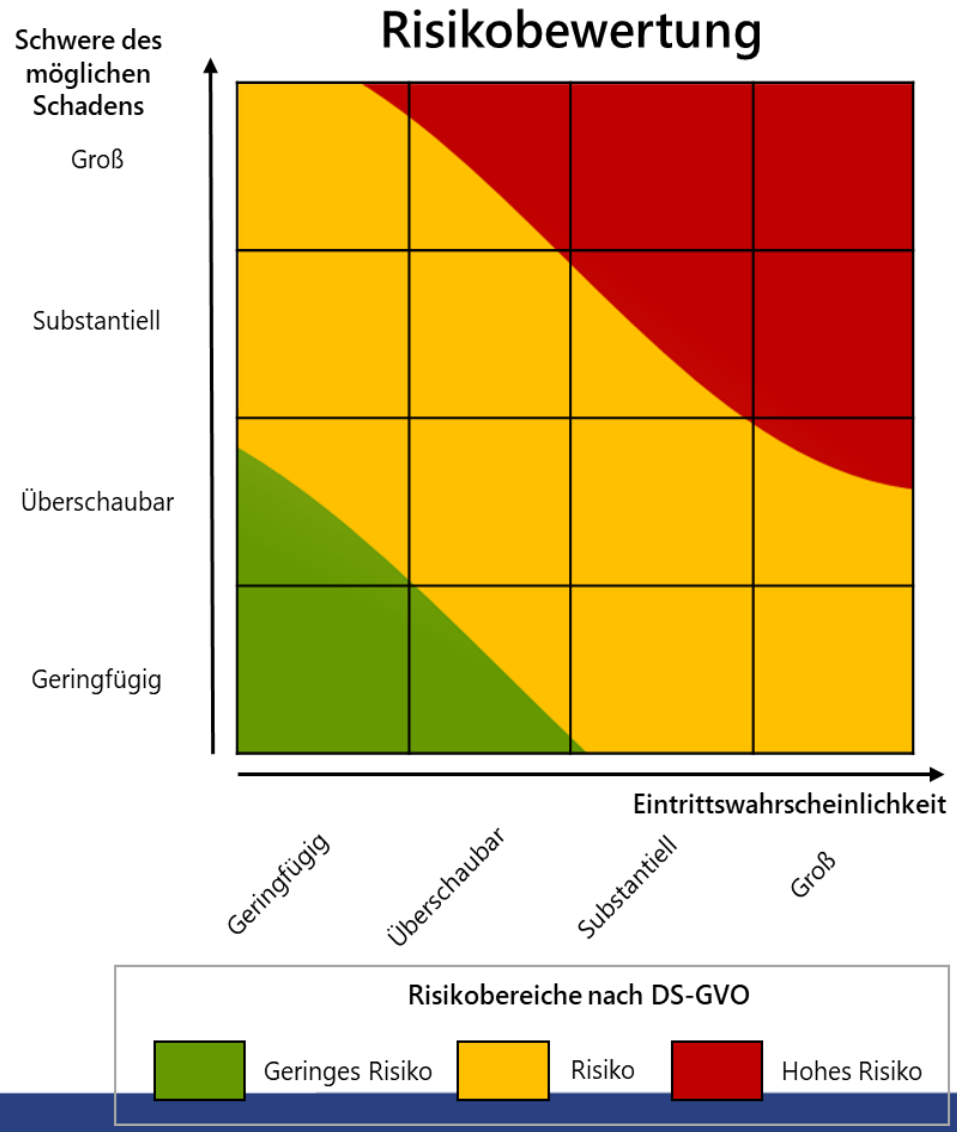
Faktoren der Risikobeurteilung

- Schwere möglicher Schäden
  - Wesentliche Faktoren:
    - Schützenswerte Personen/Daten (Kinder, Beschäftigte, Artt. 9, 10)
    - Eindeutig identifizierende Daten, zB PKZ
    - Profiling
    - Reversibilität des Schadens
    - Systematische Überwachung
    - Anzahl der Personen, Datensätze, Merkmale in Datensatz oder geographische Abdeckung

Zuordnung zu Risikoabstufungen

- Kategorisierung als Vorschlag
- Kurven sind Feature: verdeutlicht Grenzfälle
  - Verantwortung für Entscheidung bei Verantwortlicher
  - Muss sachlich begründet/ dokumentiert/prüfbar sein

Abschätzung d. Restrisikos nicht vergessen!



Technische und organisatorische Maßnahmen

An mehreren Stellen der DSGVO gefordert:

- **Art. 24: „Verantwortung des Verantwortlichen"**
  - muss Nachweis erbringen, dass er Datenschutzmaßnahmen ergriffen hat und sich an die Vorgaben der DSGVO hält.
- **Art. 25: „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen"**
  - proaktiver Datenschutz, mit Blick auf die Beeinträchtigung der Rechte und Freiheiten Betroffener, gefordert.
- **Art. 30: Verzeichnis der Verarbeitungstätigkeiten für den Verantwortlichen sowie des Auftragverarbeiters**
- **Art. 32: Sicherheit der Verarbeitung**
  - gefordert wird u.a. ein Verfahren zur dauerhaften Überprüfung von Datenschutz → Datenschutzmanagement
- **Art. 35: Datenschutz-Folgenabschätzung**
  - Verfahren mit „hohem Risiko" müssen vor Produktivsetzung auf wirksame Umsetzung der Anforderungen hin geprüft werden.

Zusammenspiel von IT Security und Datenschutz

Operative Lösung des DS-Rechts in Deutschland ist das **Standard-Datenschutz-Modell (SDM)**

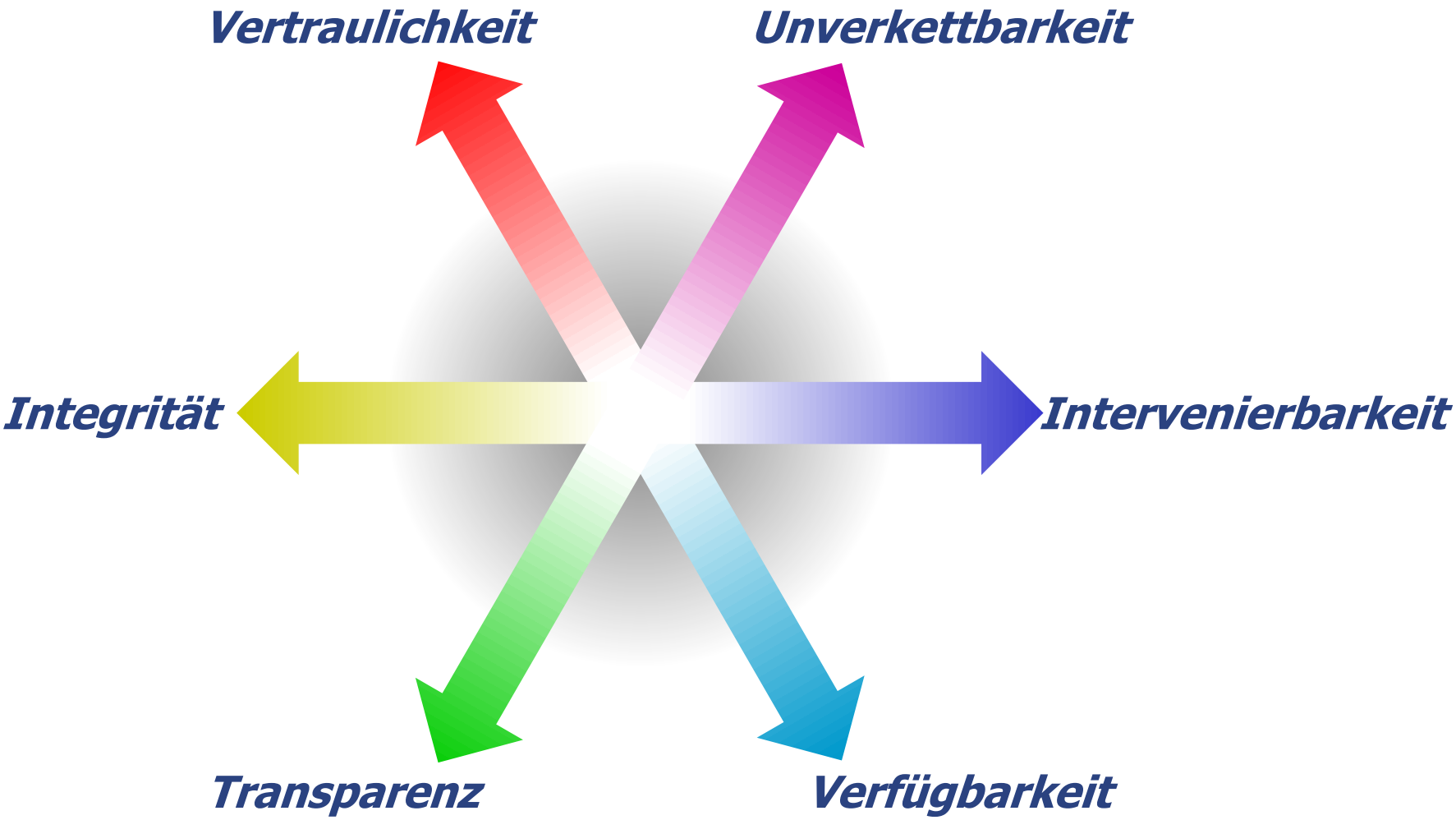
- Basiert auf 6 Gewährleistungszielen (Schutzziele), die helfen sollen, geeignete TO Maßnahmen zu finden:
  - Vertraulichkeit, Integrität, Verfügbarkeit
  - Nichtverkettbarkeit, Transparenz, Intervenierbarkeit

Prüfung in Verfahren: Daten, Systeme, Prozesse

These:

- Für die Bestimmung von TO Maßnahmen kann man **Erfahrungen aus IT Sicherheit + Cybersecurity nutzen und so Synergien schaffen.**

Standarddatenschutzmodell (SDM) und Gewährleistungsziele



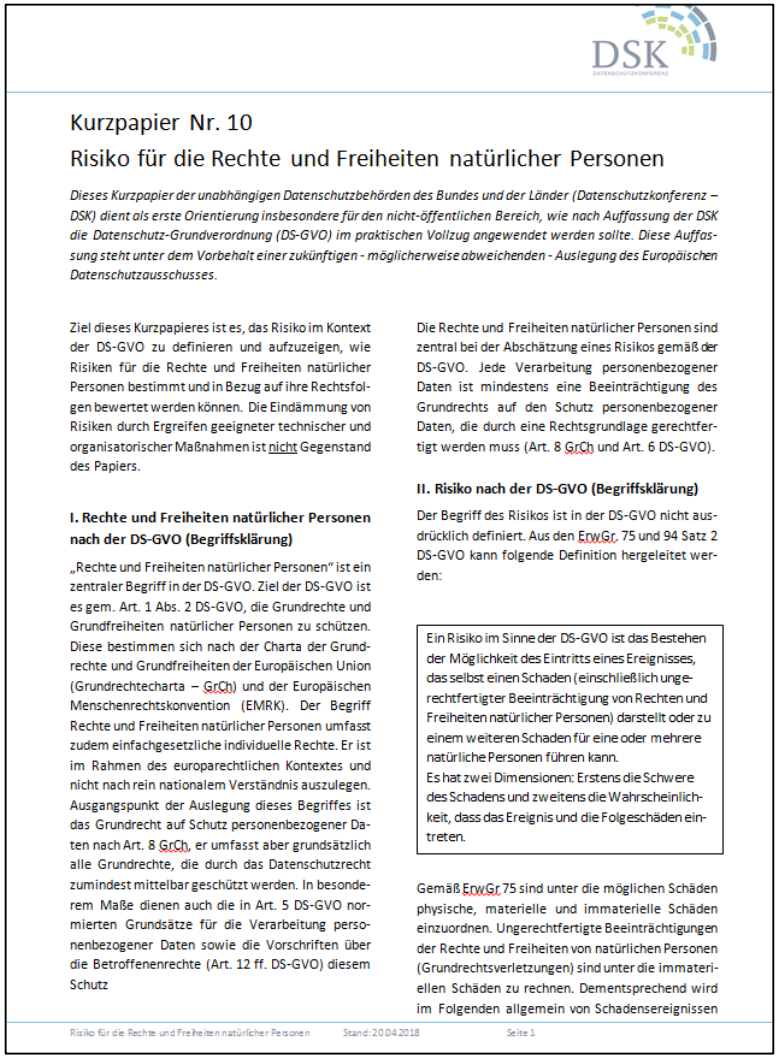
Aktueller Stand

Derzeit noch alte Fassung verfügbar, aber Update des SDM ist derzeit in Bearbeitung.

Wird 2018 kommen, ebenso wie verbesserte englische Fassung.

Ebenfalls im Erscheinen:

Kurzpapier der DSK zu „Risiko“ Datenschutzsicht



DSK

Kurzpapier Nr. 10

Risiko für die Rechte und Freiheiten natürlicher Personen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Ziel dieses Kurzpapieres ist es, das Risiko im Kontext der DS-GVO zu definieren und aufzuzeigen, wie Risiken für die Rechte und Freiheiten natürlicher Personen bestimmt und in Bezug auf ihre Rechtsfolgen bewertet werden können. Die Eindämmung von Risiken durch Ergreifen geeigneter technischer und organisatorischer Maßnahmen ist nicht Gegenstand des Papiers.

I. Rechte und Freiheiten natürlicher Personen nach der DS-GVO (Begriffsklärung)

„Rechte und Freiheiten natürlicher Personen“ ist ein zentraler Begriff in der DS-GVO. Ziel der DS-GVO ist es gem. Art. 1 Abs. 2 DS-GVO, die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen. Diese bestimmen sich nach der Charta der Grundrechte und Grundfreiheiten der Europäischen Union (Grundrechtecharta – GrCh) und der Europäischen Menschenrechtskonvention (EMRK). Der Begriff Rechte und Freiheiten natürlicher Personen umfasst zudem einfachgesetzliche individuelle Rechte. Er ist im Rahmen des europarechtlichen Kontextes und nicht nach rein nationalem Verständnis auszulegen. Ausgangspunkt der Auslegung dieses Begriffes ist das Grundrecht auf Schutz personenbezogener Daten nach Art. 8 GrCh, er umfasst aber grundsätzlich alle Grundrechte, die durch das Datenschutzrecht zumindest mittelbar geschützt werden. In besonderem Maße dienen auch die in Art. 5 DS-GVO normierten Grundsätze für die Verarbeitung personenbezogener Daten sowie die Vorschriften über die Betroffenenrechte (Art. 12 ff. DS-GVO) diesem Schutz

Die Rechte und Freiheiten natürlicher Personen sind zentral bei der Abschätzung eines Risikos gemäß der DS-GVO. Jede Verarbeitung personenbezogener Daten ist mindestens eine Beeinträchtigung des Grundrechts auf den Schutz personenbezogener Daten, die durch eine Rechtsgrundlage gerechtfertigt werden muss (Art. 8 GrCh und Art. 6 DS-GVO).

II. Risiko nach der DS-GVO (Begriffsklärung)

Der Begriff des Risikos ist in der DS-GVO nicht ausdrücklich definiert. Aus den ErwGr. 75 und 94 Satz 2 DS-GVO kann folgende Definition hergeleitet werden:

> Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.
> Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.

Gemäß ErwGr 75 sind unter die möglichen Schäden physische, materielle und immaterielle Schäden einzuordnen. Ungerechtfertigte Beeinträchtigungen der Rechte und Freiheiten von natürlichen Personen (Grundrechtsverletzungen) sind unter die immateriellen Schäden zu rechnen. Dementsprechend wird im Folgenden allgemein von Schadensereignissen

Risiko für die Rechte und Freiheiten natürlicher Personen Stand: 20.04.2018 Seite 1

Förderhinweis

Die in diesem Vortrag vorgestellten Erkenntnisse basieren auf Arbeit der folgenden Forschungsprojekte:

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

www.forum-privatheit.de/

SPECIAL

specialprivacy.eu

Privacy & Us

www.privacyus.eu

CANVAS

https://canvas-project.eu

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Horizon 2020
European Union funding
for Research & Innovation

Für das Projekt **SPECIAL** (Scalable Policy-awarE linked data arChitecture for prIvacy, trAnsparency and compliance) wurden im Rahmen der Finanzhilfevereinbarung Nr. 731601 Fördermittel aus dem Programm der Europäischen Union für Forschung und Innovation "Horizon 2020" bereit gestellt.

Für das Projekt **Privacy&Us** wurden Fördermittel aus dem Programm der Europäischen Union für Forschung und Innovation "Horizon 2020" unter dem Marie Skłodowska-Curie grant agreement Nr. 675730 im Rahmenprogramm des Marie Skłodowska-Curie Innovative Training Networks (ITN-ETN) bereit gestellt.

Für das Projekt **CANVAS** (Constructing an Alliance for Value-driven Cybersecurity) wurden im Rahmen der Finanzhilfevereinbarung Nr. 700540 Fördermittel aus dem Programm der Europäischen Union für Forschung und Innovation "Horizon 2020" bereit gestellt.

Vielen Dank für Ihre Aufmerksamkeit!

Eva Schlehahn

uld67@datenschutzzentrum.de

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstraße 98, 24103 Kiel
0431 988 1200
mail@datenschutzzentrum.de

Literatur, Referenzen

- Alexy, Robert, 2003: **Die Gewichtsformel**, in: Jickeli, J.; Kreutz, P.; Reuter, D., 2003: Gedächtnisschrift für Jürgen Sonnenschein, Berlin, De Gruyter Verlag: 777ff.
- Bieker, Felix, 2018: **Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell**, in DuD (Datenschutz und Datensicherheit) Januar 2018, Volume 42, Issue 1, pp 27–31.
- DSBK 2016: **Standard-Datenschutzmodell**, Handbuch, V1.0 (herunterladbar von Webservern der deutschen Datenschutzaufsichtsbehörden, https://www.datenschutz-mv.de/datenschutz/sdm/SDM-Methode_V_1_0.pdf).
- Rost, Martin, 1997: Zur Krise der Hochschule - **Über die Industrialisierung der Wissenschaft** - die Informations-gesellschaft als Vollendung des industriellen Projekts; in: Bulmahn, Edelgard (Hrsg.), 1997: Hochschulen in der Informationsgesellschaft - Initiative "Informationsgesellschaft - Medien - Demokratie", Berlin: 11-20.
- Rost, Martin, 2013: **Zur Soziologie des Datenschutzes**; in: DuD - Datenschutz und Datensicherheit, 37. Jg, Heft 2: 85-91.
- Rost, Martin; Storf, Katalin, 2013: **Zur Konditionierung von Technik und Recht mittels Schutzzielen**; in: Horbach, Matthias (Hrsg.), 2013: Informatik 2013 - Informatik angepasst an Mensch, Organisation und Umwelt, 16.-20. September 2013, Koblenz, Lecture Notes in Informatics (LNI) - Proceedings, Series of the Gesellschaft für Informatik e.V. (GI), Volume P-220: 2149-2166.
- Rost, Martin, 2013: **Eine kurze Geschichte des Prüfens**; in: BSI 2013: Informationssicherheit stärken, Vertrauen in die Zukunft schaffen, Tagungsband zum 13. Deutschen IT-Sicherheitskongress, Gau Algesheim, Secumedia: 25-35.
- Rost, Martin, 2014: **9 Thesen zum Datenschutz;** in: Pohle, Jörg; Knaut, Andrea (Hsrg), 2014: Fundationes I: Geschichte und Theorie des Datenschutzes.
- Rost, Martin, 2017: **Organisationen grundrechtskonform mit dem Standard-Datenschutzmodell gestalten;** in: Sowa, Aleksandra (Hrsg.), 2017: IT-Prüfung, Sicherheitsaudit und Datenschutzmodell, neue Ansätze für die IT-Revision, Wiesbaden, Springer Vieweg: 23-56.
- Rost, Martin, 2017: **Bob, es ist Bob!** FiFF-Kommunikation, 34. Jahrgang, Nr. 4: 63-66.