Datenschutzrecht

CAU

Medizindatenschutz, Berufsgeheimnisträger

Aktuelle Fragen aus der Datenschutzforschung: Transparency enhancing Technologies (TETs), Schlüsselmanagement

10. Dezember 2018

Harald Zwingelberg

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Wiederholung

Grundregeln

Wiederholung
Sechs Goldene Regeln des Datenschutzes

Welche Grundsätze des Datenschutzes kennen Sie?

- Rechtmäßigkeit
  - Gesetz, Einwilligung, Vertrag, Dienst- oder Betriebsvereinbarung
- Zweckbindung
  - Verwendung nur für Erhebungszweck
- Datenminimierung und Speicherbegrenzung
  - Verarbeitung nur soweit für Erhebungszweck erforderlich
- Transparenz und Betroffenenrechte
  - Unterrichtung über Verwendung, Auskunfts-/Berichtigungs-/Löschrechte
- Datensicherheit und Richtigkeit
  - Technische und organisatorische Maßnahmen, Integrität und Vertraulichkeit
- Kontrolle
  - Interner / externer Datenschutzbeauftragter

Wiederholung

- Wo sind die Grundprinzipien des Datenschutzes geregelt?
  - Art. 5 DSGVO

- Nennen sie die Grundprinzipien und deren Kerninhalt
  1. Rechtmäßigkeit, Art. 5 I a
  2. Zweckbindung, Art. 5. I b
  3. Erforderlichkeit, Art. 5 I b, c
  4. Transparenz, Art. 5 I a
  5. Integrität und Vertraulichkeit (Datensicherheit), Art. 5 I f
  6. Kontrolle, Art. 5 II

Wiederholung
Art. 6 DSGVO: Zentrale Befugnisnorm

- Datenverarbeitung ist nur (!) rechtmäßig, wenn:
  - **Einwilligung**
  - **Vertragserfüllung**
  - **Erfüllung rechtlicher Verpflichtung**
  - Lebenswichtige Interessen
  - Ausübung öffentliche Gewalt
  - **Wahrung berechtigter Interessen (sofern Interessen des Betroffenen nicht überwiegen)**

Ausführlich zur Verarbeitung für berechtigte Interessen nach Art. 6 I f DSGVO:
Robrahn/Bremert, Interessenskonflikte im Datenschutzrecht, ZD 2018, 291ff.
(Beruhend auf Forschungen mit Förderungen des BMBF in den Projekten SeDaFa und iTESA)

iTESA

SeDaFa
Selbstdatenschutz im vernetzten Fahrzeug

Gesundheitsdatenschutz

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Medizin- und Sozialdatenschutz

1. Geheimnisschutz
2. Gesetzesgrundlagen, Datenerhebung
3. Einwilligung – Schweigepflichtsentbindungserklärung
4. Zweckbindung und Erforderlichkeit
5. Datenübermittlung
6. Betroffenenrechte, insbesondere Akteneinsichtsrechte
7. Datensicherheit
8. Kontrolle

Fragen

- Patientendaten beim Arzt und Versichertendaten bei den Sozialversicherungen unterliegen einem besonderen Schutz. Welche Gründe könnte es dafür geben? Wer hat ein Interesse an diesem Schutz?

- Welche Sozialversicherungsträger (Sozialversicherungen) kennen Sie?

- Welche Gründe kann es geben Daten bei Sozialversicherungsträgern besonders zu schützen?

Gründe für Schweigepflicht und Sozialgeheimnis

Ärztliche Schweigepflicht

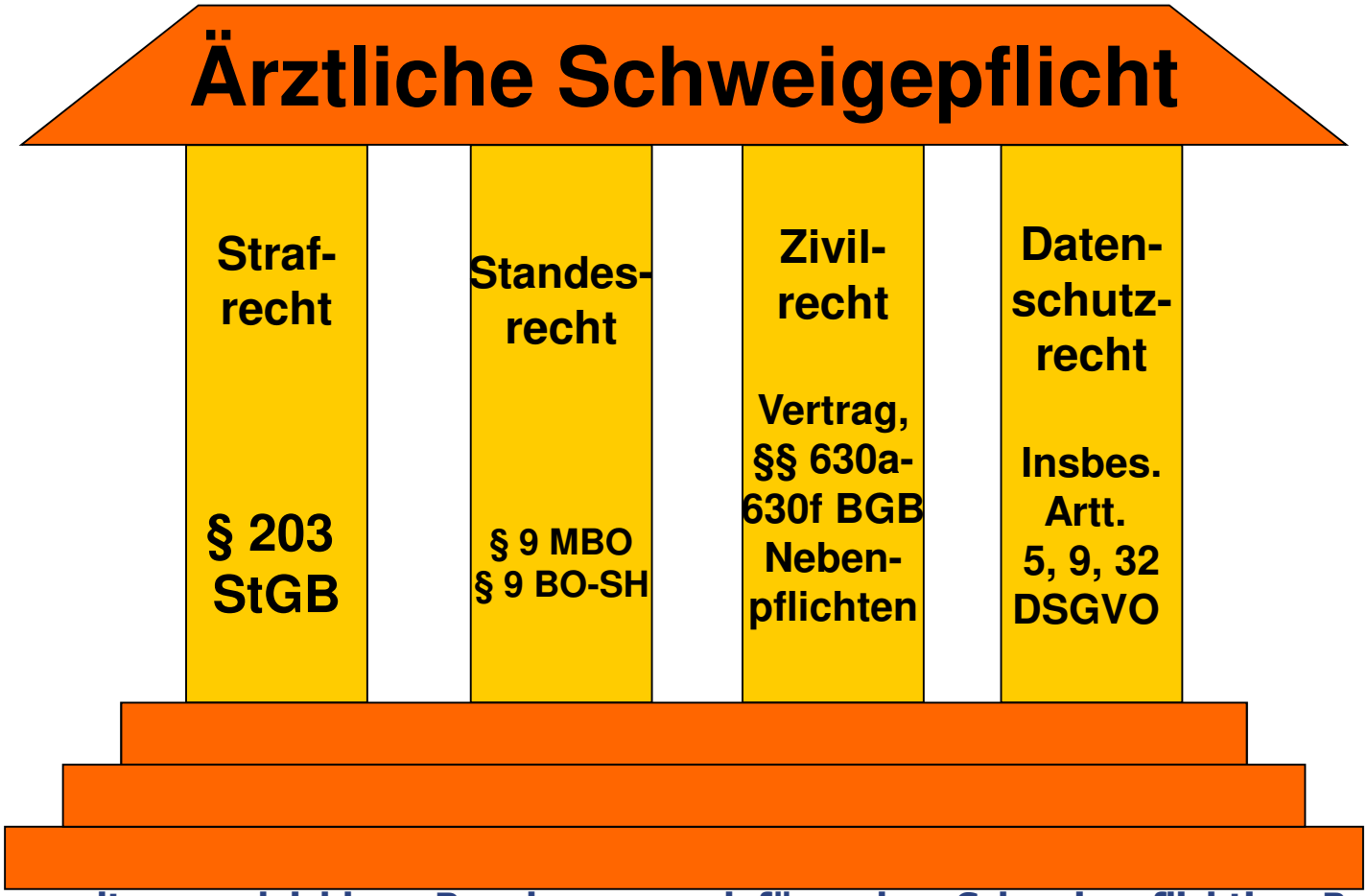
- Persönlichkeitsrecht des Patienten
- staatliches Interesse an gesunden Bürgern und Vertrauen in die Vertraulichkeit der Arzt-Patientenbeziehung
- Eigeninteresse der Ärzte – Vertrauen der Patienten (therapeutisch und wirtschaftlich – siehe Erläuterungen zum Hippokratischen Eid)
- besonders schutzbedürftige Daten

Sozialgeheimnis

- Persönlichkeitsrecht des Betroffenen
- staatliches Interesse an der Vermeidung sozialer Notlagen
- Angehörige einer Sozialversicherung (ob zwangsweise oder freiwillig) sollen nicht mehr staatlichen Eingriffen ausgesetzt sein als andere
- besonders schutzbedürftige Daten (insbes. Gesundheit, Vermögen, soziale Verhältnisse)

Beachte: Auch Datenschutzrechtlich unterliegen Gesundheitsdaten als eine Art von besonders sensitiven Daten nach § 9 DSGVO besonderen datenschutzrechtlichen Anforderungen. Im Sozialrecht finden sich diese im SGB X.

Grundlagen der ärztlichen Schweigepflicht*



*** im Kern gelten vergleichbare Regelungen auch für andere Schweigepflichtige: Beamte bezüglich Amtsgeheimnissen, Rechtsanwälte, Steuerberater, Geistliche, … Unterschiede bestehen bezüglich der anwendbaren Rechtsgrundlagen.**

Umfang und Adressatenkreis der ärztlichen Schweigepflicht

§ 203 StGB: Verletzung von Privatgeheimnissen

- Adressatenkreis: u.a. Ärzte, Zahnärzte, Tierärzte, Heilberufe mit staatl. Prüfung, Psychologen, Rechtsanwälte, Notare, Steuerberater, Ehe- Familien Jugendberater, Mitglieder von Beratungsstellen, Sozialarbeiter, Mitarbeiter privater Krankenkassen bzw. Unfall- oder Lebensversicherungen,
  Umfang: Bereits die Tatsache, dass jemand Patient ist
- „unbefugte" Offenbarung eines fremden Geheimnisses
  - Keine Mitteilung an Familienmitglieder der Patienten
  - Schweigepflicht gilt idR über den Tod des Patienten hinaus
  - Rechtfertigung der Geheimnisoffenbarung durch
    - Einwilligung
    - Mutmaßliche Einwilligung (z.B. bei Bewusstlosen)
    - Gesetzliche Offenbarungspflichten (z.B. § 138 StGB)
    - Rechtfertigender Notstand (z.B. § 34 StGB)

Grenzen der Schweigepflicht: Beispiele

- Bankräuber beim Arzt: Pflicht zur Anzeige nur bei bestimmten geplanten (künftigen) Straftaten (vgl. § 138 StGB). Im Übrigen: Schweigepflicht
- Misshandeltes Kind beim Arzt: § 34 StGB – Recht zur Benachrichtigung der zuständigen Stelle, z.B. des Jugendamtes, aber keine Mitteilungspflicht
- Alkoholiker fährt regelmäßig Auto: Mitteilung an Register? § 34 StGB
- Einschaltung externer Inkassounternehmen bei der Behandlungsabrechnung als Auftragsverarbeiter denkbar (siehe unten)
- HIV-Patient beim Arzt: Pflicht zur Mitteilung der HIV-Infektion an den/die Sexualpartner(in)? § 34 StGB bei Anhaltspunkten für eine *konkrete* Ansteckungsgefahr (z.B. erklärte Absicht des Patient zu ungeschütztem Geschlechtsverkehr mit einer bestimmten Person) (so ein sehr umstrittenes - und nach allg. Meinung falsches - Urteil des OLG Frankfurt)
- Arzthaftungsprozess: Mitteilung von Patientendaten zur rechtlichen Verteidigung? Nach § 34 StGB zulässig, aber nur im erforderlichen Umfang
- Polizei fahndet nach einem Bankräuber und befragt den Arzt, bei dem dieser in Behandlung war: Schweigepflicht

Rechtliche Bedeutung der Schweigepflicht

- Verfassungsrechtliche Ausgangslage: Dem Bürger ist alles erlaubt, was nicht verboten ist (Art. 2 Abs. 1 GG: Recht auf freie Entfaltung der Persönlichkeit, insb. allgemeine Handlungsfreiheit).
- Im Datenschutz gilt aber auch für Private: Alles ist verboten, was nicht erlaubt ist (Art. 6 (1) und Art. 5 (1) (a) DSGVO). – Jeder Umgang mit personenbezogenen Daten bedarf einer rechtlichen Grundlage. [Stichwort: Rechtmäßigkeit]

- In Bereichen, die einem besonderen Geheimnisschutz unterstellt sind (neben der ärztlichen Schweigepflicht und dem Sozialgeheimnis etwa auch das Steuergeheimnis) werden an die rechtlichen Grundlagen besondere Anforderungen gestellt: Daten dürfen nur dann erhoben, verarbeitet und übermittelt werden, wenn ***bereichsspezifische*** Regelungen dies erlauben.
  Also bei besonderem Verbot braucht es auch eine solche Ausnahme.

Sozialgeheimnis

- § 35 Abs. 1 Satz 1 SGB I – Sozialgeheimnis:
- Berechtigter: „Jeder" (über den Sozialdaten erhoben werden) Leistungsempfänger, Vermieter, Arbeitgeber,...
- Adressat: alle Leistungsträger (nicht Leistungserbringer wie z.B. Ärzte)

  => Institutionenbezogenes Spezialrecht für Leistungsträger
- Klarstellung: Auch innerhalb eines Leistungsträgers dürfen Daten nur Befugten zugänglich sein, § 35 I SGB I

- Gegenstand: Sozialdaten nach § 67 Abs. 1 SGB X

  „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener)"
- Normbefehl:
  - Verbot „unbefugter" Datenverarbeitung
  - § 35 II SGB I: nur nach den Voraussetzungen der §§ 67 ff. SGB X

Erhebung von Sozialdaten, § 67a SGB X

- Grundsatz: Sozialdaten dürfen erhoben werden, wenn sie zur Aufgabenerfüllung erforderlich sind
  - Keine Datenerhebung auf Vorrat
  - Nur entscheidungserhebliche Tatsachen
  - Daten müssen auch tatsächlich Verwendung finden
  - Kontoauszüge: Vorlagepflicht für Auszüge der vergangenen 3 Monate, Schwärzung bei bes. Arten personenbezogenen Daten statthaft. § 67a I 2, i.V.m. § 67 XII SGB X

Zu Kontoauszügen siehe: BSG, Urteil vom 19. 9. 2008 - B 14 AS 45/ 07 R ; und unter:
https://www.datenschutzzentrum.de/sozialdatenschutz/faq-sozialamt/#11

Erhebung von Sozialdaten, § 67a SGB X

- Es gilt der Grundsatz der Datenerhebung beim Betroffenen

- Transparenz: Betroffener muss bei Erhebung über den Zweck der Erhebung und Verarbeitung, die verantwortliche Stelle und die relevanten Rechtsvorschriften informiert werden.

- Hinweis auf Rechtsfolgen: Soweit eine Auskunftspflicht besteht oder bei Nichtauskunft Nachteile drohen, ist darauf hinzuweisen.
  (Auskunftspflicht z.B. in § 60 SGB I, Folgen § 66 SGB I)

Einwilligung in eine medizinische Untersuchung

Medizinrechtliche Einwilligung

- Einwilligung in den Eingriff, andernfalls ist Behandlung eine Körperverletzung
- Informed consent = Aufklärung und freie Einwilligung
- Aufklärung über
  - 1. Diagnose und Diagnosesicherheit
  - 2. Verlaufsprognose
  - 3. Wesen der Maßnahme, Mitwirkungspflichten
  - 4. Erfolgsquote, Nutzen
  - 5. Komplikationen und Komplikationswahrscheinlichkeit
  - 6. Handlungsalternativen
  - 7. Wirtschaftliche Aufklärung

- Schwerpunkt: Einwilligung in körperlichen Eingriff
- Aber auch: Einwilligung in Informationsgewinnung und übermittlung (Recht auf informationelle Selbstbestimmung und Recht auf Nichtwissen)

Datenschutzrechtliche Einwilligung:

- Informierte Einwilligung, Art. 13 DSGVO
- Anforderungen nach Art. 7 DSGVO, insb.:
  - freie Entscheidung, Art. 7 (4)
  - Aufklärung über den Zweck der Datenerhebung oder -verarbeitung Art. 13 (1) (c)
  - Keine Formpflicht aber Nachweisobliegenheit, Art. 7 (1)
  - ggf. besondere Hervorhebung der datenschutzrechtlichen Einwilligungserklärung Art. 7 (2)
  - ausdrücklicher Hinweis auf die Verwendung von Gesundheitsdaten, Art. 8 (2) (a) DSGVO
- Schwerpunkt: Schutz des Rechts auf informationelle Selbstbestimmung
- beachte z.B. § 9 Abs. 3 MBO: Hinweis auf die Daten, die aufgrund einer vermuteten Einwilligung übermittelt werden dürfen

Einwilligung - Beispielsfälle

- Heimlicher HIV-Test – unzulässig, da keine zu erwartende Routineuntersuchung
- Forschung: Forschung mit anonymisierten Daten ist zulässig, Untersuchungen an personenbezogenen Proben ohne Einwilligung sind i.d.R. unzulässig (Recht auf informationelle Selbstbestimmung und Recht auf Nichtwissen).
- Fotos von Patienten als Gedächtnisstütze für den Arzt: keine übliche Maßnahme und nicht erforderlich für Patientenakte aber mit Einwilligung der Patienten möglich. Keinesfalls darf fotografiert werden ohne vorherige Aufklärung und Einwilligung.
- Betriebsarzt: Proband muss über die Untersuchung im Vorwege aufgeklärt werden, insbesondere wenn Untersuchung nicht üblich oder erkennbare Voraussetzung für die angestrebte Tätigkeit ist.

Zweckbindung und Erforderlichkeit

- Der Zweck der Erhebung und Verarbeitung muss hinreichend bestimmt sein. Rahmen ist in der Regel das konkrete Behandlungsverhältnis
- Der Umfang der Erhebung und Verarbeitung der Daten muss erforderlich sein. (Die Erforderlichkeit wird häufig durch die gesetzgeberische Wertung sichergestellt. Gesondert geprüft werden muss sie nur dort, wo sie ausdrücklich erwähnt wird, z.B. § 28 Abs. 6 Nr. 1 BDSG.)
- Arzthaftungsprozess: Es dürfen nur Patientendaten dem RA offengelegt werden, deren Kenntnis für den Prozess erforderlich ist, Art. 9 (2) (f) DSGVO. Schwierige Bestimmung der Erforderlichkeit, weil Vor- oder Miterkrankungen u.a. für die Bestimmung der Schadenshöhe relevant sind und diese Bewertung oft nur im Dialog mit dem RA erfolgen kann.
- Forschung, Archive, Statistik: Art. 9 (2) (j) DSGVO i.V.m. nationalen Gesetzen wie § 27 BDSG-neu, §§ 13, 26 LDSG-SH-Entwurf 2018

Typische Übermittlungsbefugnisse

- Abrechnung mit der Kassenärztlichen Vereinigung
- Bei Privatliquidation ist bisher Einwilligung für Übermittlung an eine Einzugsstelle notwendig – Transparenzpflicht bleibt aber!
  neu: kein Hindernis im StGB mehr durch § 203 III 2 StGB-2017
- §§ 284 ff, 294 ff SGB V (Vertragsarztrecht)
  - Wirtschaftlichkeitsprüfungen
  - Qualitätsprüfungen z.B. Sonografie (Stichproben)
- Meldepflichten: InfektionsschutzG, KrebsregisterG
- Bei vor-, mit und nachbehandelnden Ärzten wird konkludente Einwilligung unterstellt - d.h. Widerspruch ist möglich, § 9 MBO
- Praxisinterne Übermittlung, gegenseitige Einsicht in Patientenakten:
  (+) Gemeinschaftspraxis (Partner, Gesellschaft), MVZ,
  (-) Praxisgemeinschaft (gemeinsam genutzte Räume und Mitarbeiter), angegliederte Kosmetikerin beim Dermatologen
- Klinken: Meldeschein Hotel zur Einsicht der Polizei, wie bei Hotel

Auftragsverarbeitung im Bereich des § 203 StGB

- Auftragsverarbeitung ist auch für Berufsgeheimnisträger möglich. (Änderung aus 2017, davor war es schwierig)
- § 203 III 2 StGB:

  [2]Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist;…
- Rechtsfolge: Auftragsverarbeitung ist straffrei möglich. Es ist aber keine Rechtsgrundlage.
- Anforderungen des Art. 26 DSGVO müssen erfüllt sein. Insbesondere dem Risiko angemessene techn.-organisat. Maßnahmen, vergl. Art. 32 (2) i.V.m. Art. 28 (3) (c) DSGVO

Übermittlung von Sozialdaten, §§ 67d ff SGB X

- Übermittlung Grundsatz: Es bedarf einer **gesonderten Übermittlungsbefugnis**, die von der übermittelnden Stelle zu prüfen ist. Soweit eine andere Stelle anfragt, trägt diese die Verantwortung für die Richtigkeit der Anfrage, §_67d II SGB X

- diverse Übermittlungsbefugnisse in §§ 68-77 SGB X und anderen Sonderregelungen, z.B. für den Datenabgleich gegen Sozialleistungsmissbrauch und Schwarzarbeit

- Bei erhobenen medizinischen Daten Weitergabe nur, wenn sie dem Arzt selbst gestattet gewesen wäre, § 76 I SGB X

Betroffenenrechte im Medizinbereich

medizinrechtliche Ansprüche

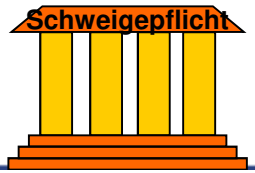
- Medizinrechtlicher Auskunftsanspruch aus Art. 2 I i.V.m. Art. 1 I GG
  - Patientenautonomie als Ausprägung des Rechts auf freie Entfaltung der Persönlichkeit
- Einsicht in Patientenakte:
  - § 630g BGB als Teil des Behandlungsvertrags
  - § 10 II Berufsordnung Ärzte
- Alle objektive Befunde unterliegen dem Einsichtsrecht. Arzt darf aber persönliche Notizen schwärzen.

datenschutzrechtliche Ansprüche

- Art. 13, 14 DSGVO Benachrichtigung
- Art. 15 DSGVO Auskunft
- Art. 17 DSGVO Löschung
- Art. 18 DSGVO Sperrung

- Zusätzlich: Schadensersatzanspruch

Für den Sozialdatenschutz finden sich entsprechende Regelungen in den §§ 84 ff. SGB X



Datensicherheit im Gesundheitsbereich

- Gesundheitsdaten sind besondere Arten von Daten und unterliegen je nach datenverarbeitender Stelle besonderer Berufsgeheimnisse.
- Es sind die **geeigneten** Maßnahmen zu treffen mit Rücksicht u.a. auf das **Risiko für die Betroffenen**.
- Umfang hängt von Quantität und Qualität der Daten ab, insbesondere welche Einschnitte Betroffene bei einem Datenverlust erleiden würden.
- Arzt hat dabei sicherzustellen:
  - Vertraulichkeit — Keine Einsicht durch Dritte
  - Verfügbarkeit — Dokumentation, Folgebehandlungen
  - Integrität — Aufbewahrungsfirsten

Auftragsverarbeitung

- Bis 2017 war Auftragsverarbeitung für Berufsgeheimnisträger nur in Ausnahmefällen (Ländergesetze) möglich oder auf Grund einer Einwilligung.
- Seit 2017: § 203 Abs. 3 StGB:

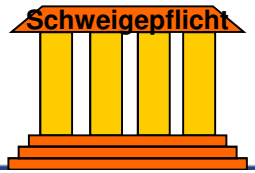
  Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.
- Damit entfällt die Strafbarkeit
- Das ist für sich allein aber keine Erlaubnis.
- Als Rechtsgrundlage kommt dann eine Auftragsverarbeitung nach der DSGVO in Betracht.

Auftragsverarbeitung

- Besondere Anforderungen an die Auftragsverarbeitung im Gesundheitsbereich:
  - Zwingende Bekanntgabe der Identitäten der Auftragsverarbeiter, Zwecke, Umfang der Verarbeitung vor Beginn der Behandlung
  - Besonders sorgfältige Auswahl aller Auftragsverarbeiter.
  - Klare Verpflichtung auf die Verschwiegenheit zwingend – Auftragnehmer muss alle eingesetzten Mitarbeiter verpflichten.
  - Soweit möglich müssen Betroffene einzelnen Verarbeitungen widersprechen können – Praktisch nicht möglich beim Haupt-IT-Dienstleister eine Klinik, denkbar aber durchaus bei der Auswahl eines externen Medizin- oder Dentallabors.
  - Eine Auftragsverarbeitung in Drittstaaten wird oft mangels hinreichender Garantien zur Gewährleistung Datensicherheit nicht möglich sein – insbesondere gegen staatliche Zugriffe. Insoweit muss m.E. das Berufsgeheimnis gewahrt bleiben.

Kontrolle im Gesundheitsbereich

- Die Kontrolle erfolgt intern (bDSB) – i.d.R. bei Kliniken oder extern.
- Externe Kontrolle je nach rechtlicher „Säule“
  - DSGVO: Datenschutzbehörden
  - Berufsrecht: Kammern (Ärztekammer, Anwaltskammer, Notarkammer, etc.)
  - Strafrecht: Staatsanwaltschaft. Wenn ein solcher Fall beiden Aufsichtsbehörden landet, wird er an die zuständige StA abgegeben. Da § 203 StGB ein Antragsdelikt ist, muss ein Geschädigter Strafantrag stellen, § 205 StGB.
  - BGB: Patient verfolgt seine Ansprüche selbst auf dem Zivilrechtsweg.

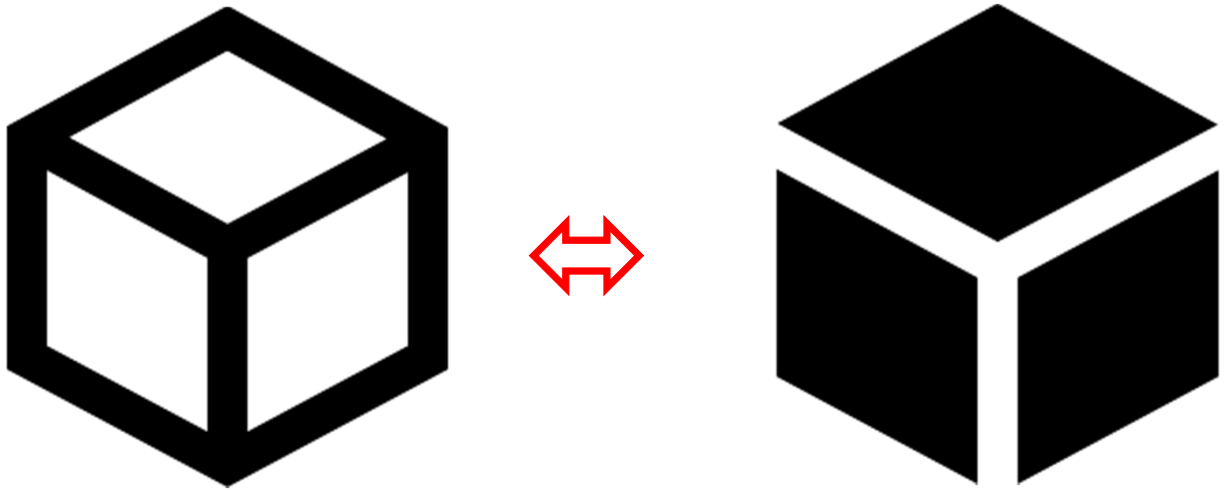


Ausgewählte Fragestellungen aus dem Projektbereich des ULD

Herstellung von Transparenz mittels Layered Policies und Transparency enhancing Technologies (TETs)

Vorab: zum Begriff Transparenz

Datenschützer ⇔ u.a. Kryptografen



In der Informatik (vor allem im US-Raum) wird Transparenz oft genau gegenteilig verstanden, nämlich als "Unsichtbarkeit" von Systemen und Prozessen um den Nutzer nicht mit Details zu belästigen

Wann Transparenz?

- Transparenz ist über den ganzen Lebenszyklus der Verarbeitungstätigkeit:
  - Planung & Dokumentation
  - Erhebung bei betroffener Person oder Drittem
  - Während der andauernden Verarbeitung
  - Zu bestimmten Zeitpunkten: z.B. bei einem data breach
  - Beim (Ver-) Kauf datenverarbeitender Devices
  - Änderung zentraler Angaben, bei Zweckänderung vorab!
  - Erinnerungsmitteilung über wesentliche Aspekte (Art. 29 WP 260 Rn. 28)
  - Nach der Löschung: Dokumentation sollte weiter verwahrt und Beleg für (sichere) Löschung

Warum Transparenz? Aus Sicht des Datenschutzrechts

- Nach DSGVO muss personenbezogene Datenverarbeitung **nachvollziehbar** sein, insbesondere in Bezug darauf,
  - welche Daten erhoben werden und in welchem Umfang
  - auf welche Art und Weise Information verarbeitet wird
  - zu welchen Zwecken und von wem

➢ Somit Umfang: Daten, Systeme, Prozesse (siehe SDM)

➢ Zwingende Vorbedingung, um Betroffenenrechte wirksam ausüben zu können (u.a. Berichtigung).

Wie?
Anforderung genereller transparenter Information und Kommunikation

Artikel 12

Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

Für wen? Adressaten

- Bei der Beurteilung, ob hinreichende Transparenz gegeben ist, ist zumeist die Perspektive des Betroffenen ausschlaggebend:
  - Art. 12 (1) …Maßnahmen, um der betroffenen Person alle Informationen […], in präziser, transparenter, verständlicher und leicht zugänglicher Form in" einfacher Sprache zu übermitteln.
  - Weitergehende Dokumentation kann sich demgegenüber an interne und externe Experten richten, und dementsprechend gefasst sein Art. 30

Informiertheit des Betroffenen (Einwilligung)

Art. 4 Nr. 11 - zusammen mit Art. 7 DSGVO - erfordert für eine wirksame Einwilligung:

- Freiwilligkeit
- Bestimmtheit (für einen oder mehrere feste Zwecke)
- Informiertheit
- Eindeutige Willensbekundung des Betroffenen
- Jederzeitige Widerrufbarkeit

Nach Art. 7 Abs. 1 DSGVO muss der Verantwortliche die wirksame Einwilligung nachweisen können!

Informiertheit des Betroffenen (Einwilligung)

- **Information**
  - Welche Daten werden verarbeitet?
  - Wer verarbeitet die Daten?
  - Zu welchem Zweck?

Art. 7 Abs. 2 DSGVO: Ersuchen um Einwilligung muss bei einer schriftlichen Erklärung, die noch andere Sachverhalte betrifft,

  - in verständlicher und leicht zugänglicher Form
  - in einer klaren und einfachen Sprache
  - von anderen Sachverhalten klar unterscheidbar sein

Zusammenfassend: Was ist Transparenz dann eigentlich?

Transparenz ist die jederzeitige Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung in Bezug auf:

- die Art der Daten,
- ihre Herkunft und Qualität,
- die Verarbeitungszwecke,
- die Umstände der Verarbeitung,
- die genutzten Systeme und Prozesse,
- die damit einhergehenden Entscheidungen
- die Rechtskonformität und
- die damit verbundenen rechtlichen Verantwortlichkeiten

Praktische Hinweise

Praktische Vorschläge für die Beratungstätigkeit

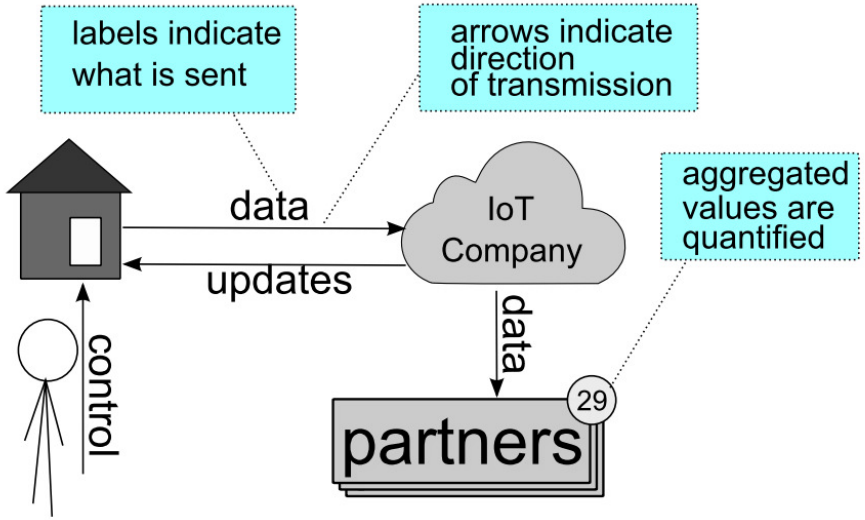
Verständlichkeit heißt weg vom Fließtext! (Art 29 WP 260 Rn. 33, 42)

- Klare Struktur des Textes
- Überschriften, Zusammenfassungen,
- Tabellen z.B. für Verarbeitern, Zwecke, Datenarten,...
- Icons (standardisierte Bildsymbole)
- Just-in-time Mitteilungen
- Übersetzungen in Landessprache der Zielgruppe (Vorsicht bei automatischer Übersetzung)
- Grafiken, wenn Datenflüsse relevant sind

Praktische Hinweise

Praktische Vorschläge

Verständlichkeit durch ergänzen von Fließtext!



- **Grafiken**, denn ein Bild sagt mehr als 1000 Worte!

Grafik in Privacy&Us D4.2 zur Veröffentlichung vorgesehen:
https://privacyus.eu/publications/deliverables/
Autor: Alexandr Railean

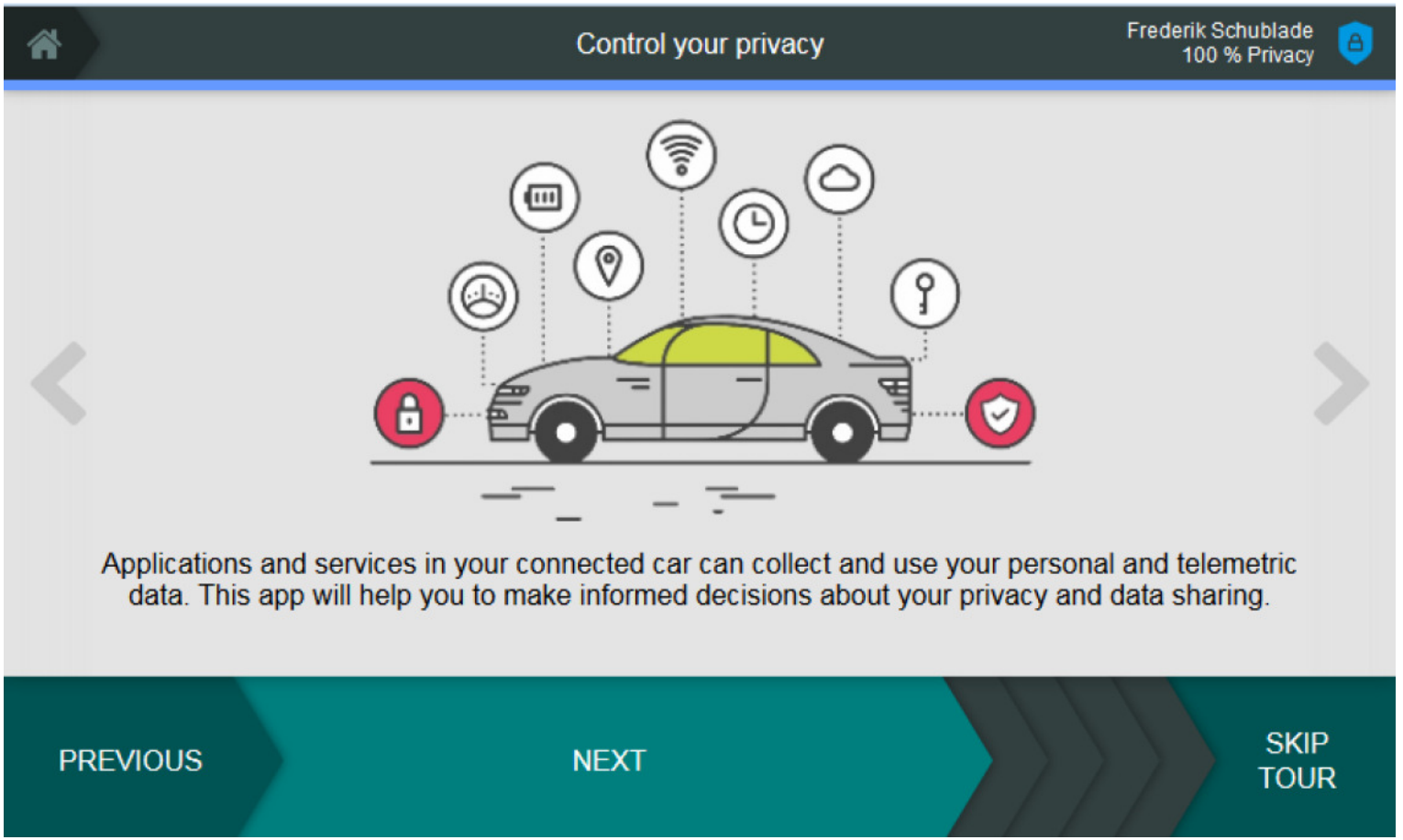
Praktische Hinweise

Praktische Vorschläge für die Beratungstätigkeit

Verständlichkeit Wichtiges vor den Fließtext ziehen!

- „Layered Policies" => Mehrstufige Erklärungen
- Schon in Art. 29 WP 100 von 2004 propagiert
- Top-Layer muss informieren, welche Angaben wo und wie gefunden werden können.
- Top-Layer kann (‚may') Informationen darüber enthalten, was den größten Einfluss auf die betroffenen Personen hat oder diese überraschen würde. D.h. Betroffene sollten Konsequenzen der Datenvearbeitung schon an Hand des ersten Layers verstehen.
  (Art. 29 WP 260 Rn. 30)

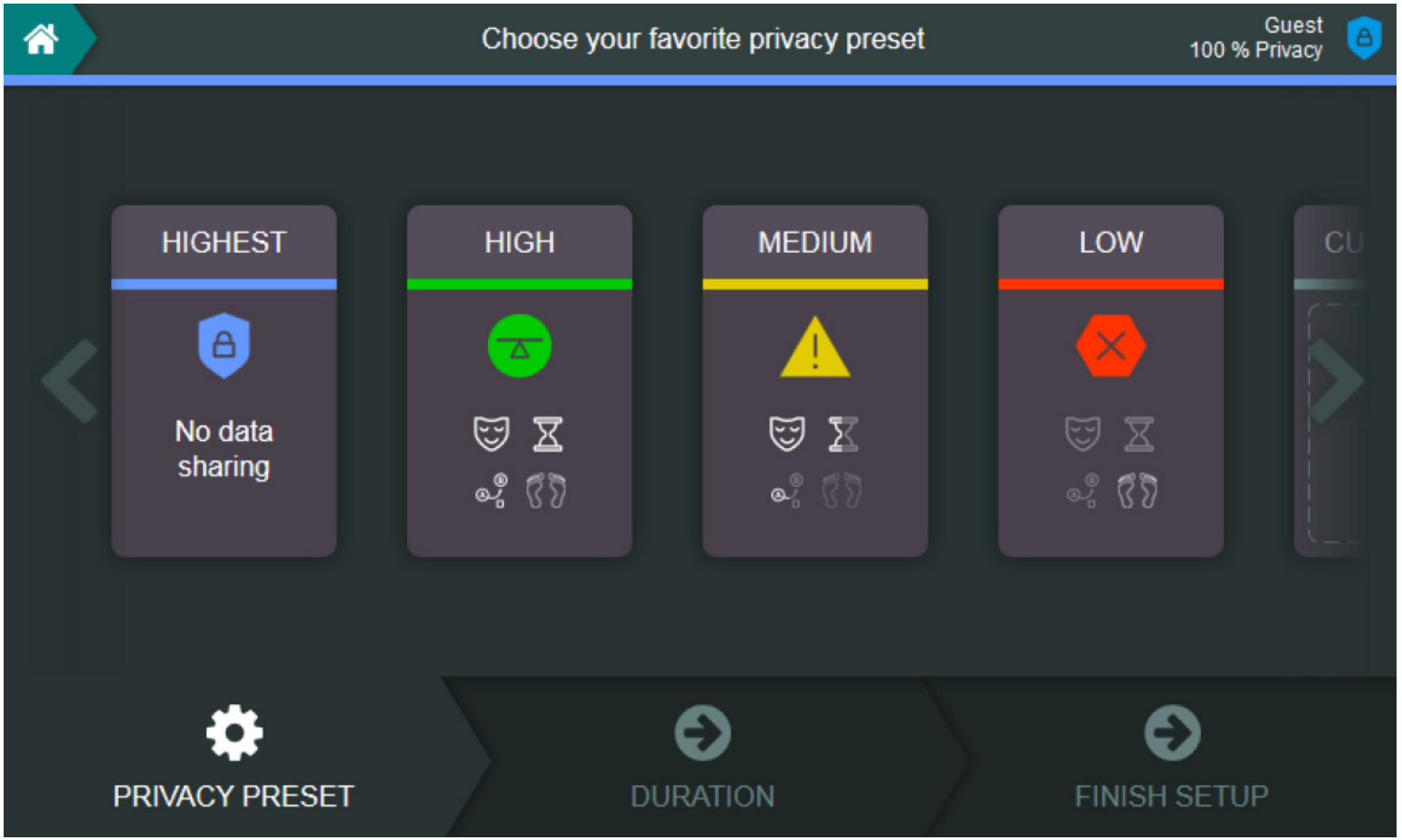
Praktische Hinweise



Grafik aus SeDaFa-Projekt, Fahrzeugbasierte Datenschutzapplikation „PRICON"

SeDaFa
Selbstdatenschutz im vernetzten Fahrzeug

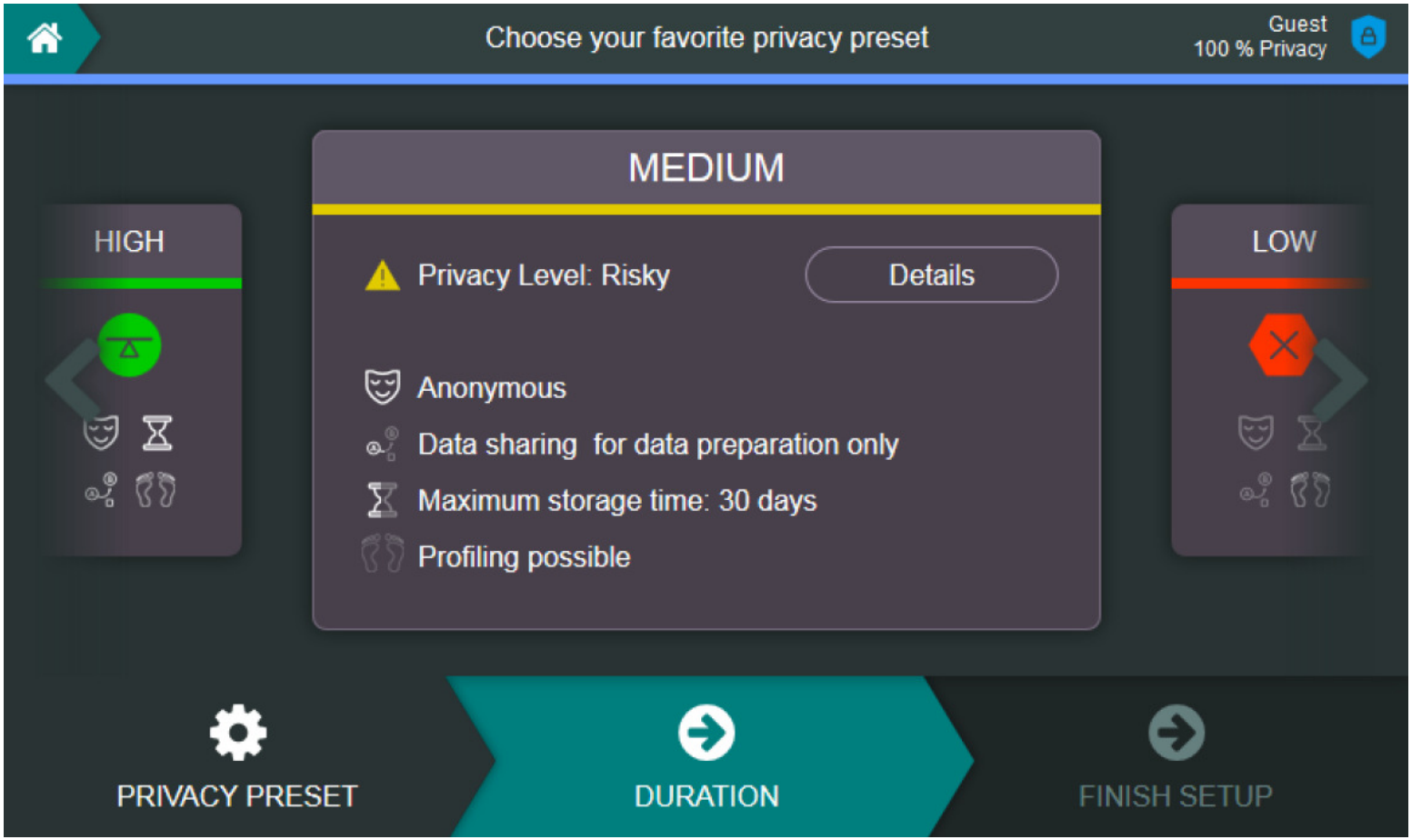
Praktische Hinweise



Grafik aus SeDaFa-Projekt, Fahrzeugbasierte Datenschutzapplikation „PRICON"

SeDaFa
Selbstdatenschutz im vernetzten Fahrzeug

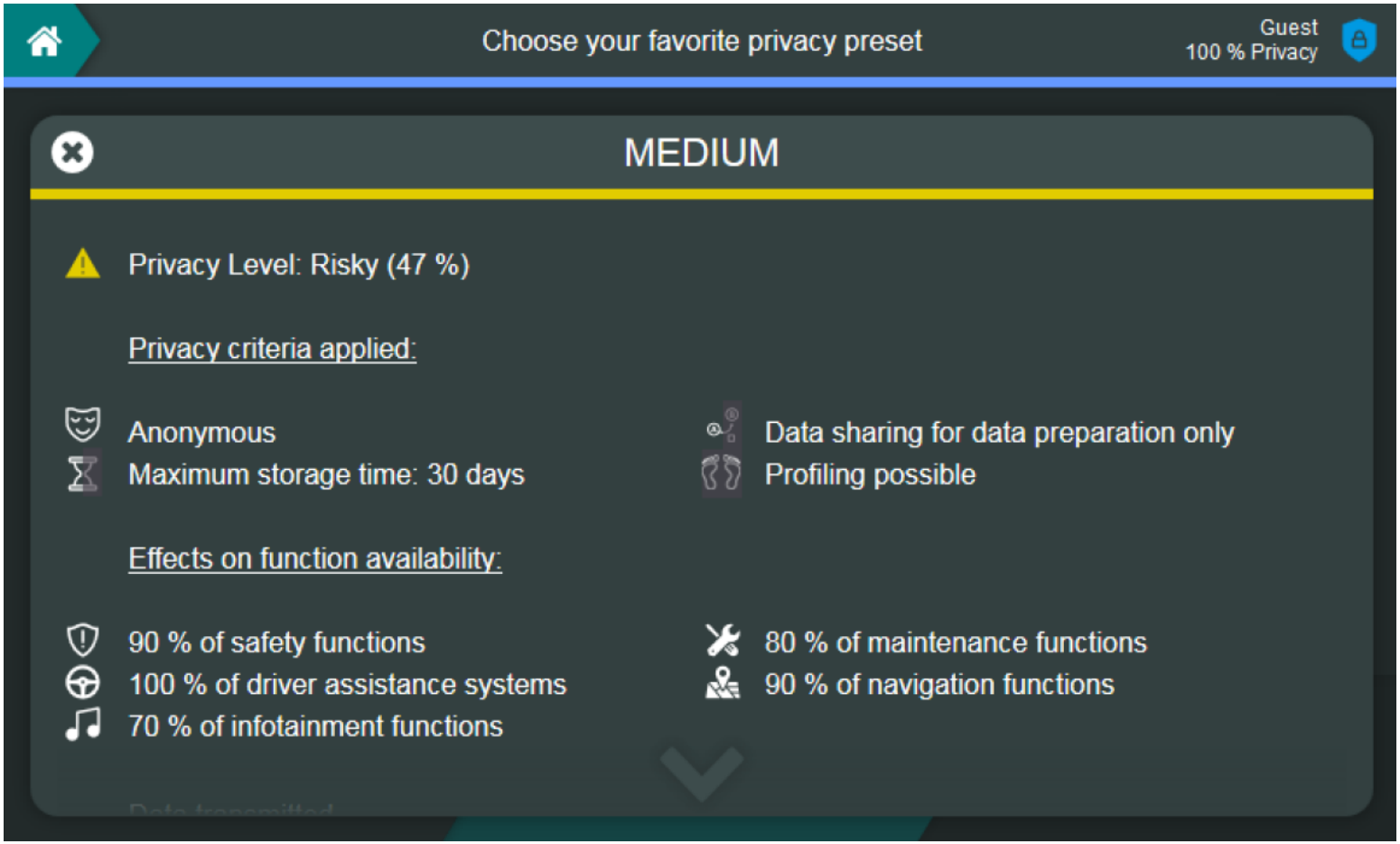
Praktische Hinweise



Grafik aus SeDaFa-Projekt, Fahrzeugbasierte Datenschutzapplikation „PRICON"

SeDaFa
Selbstdatenschutz im vernetzten Fahrzeug

Praktische Hinweise



Grafik aus SeDaFa-Projekt, Fahrzeugbasierte Datenschutzapplikation „PRICON"

SeDaFa
Selbstdatenschutz im vernetzten Fahrzeug

Praktische Hinweise

Praktische Vorschläge für die Beratungstätigkeit

Wenn es passt hilft manchmal auch ein

Medienbruch! (Art 29 WP 260 Rn. 33,)

- Telefon: Aufgezeichnete Information vorspielen mit Option, weitere Details anzuhören

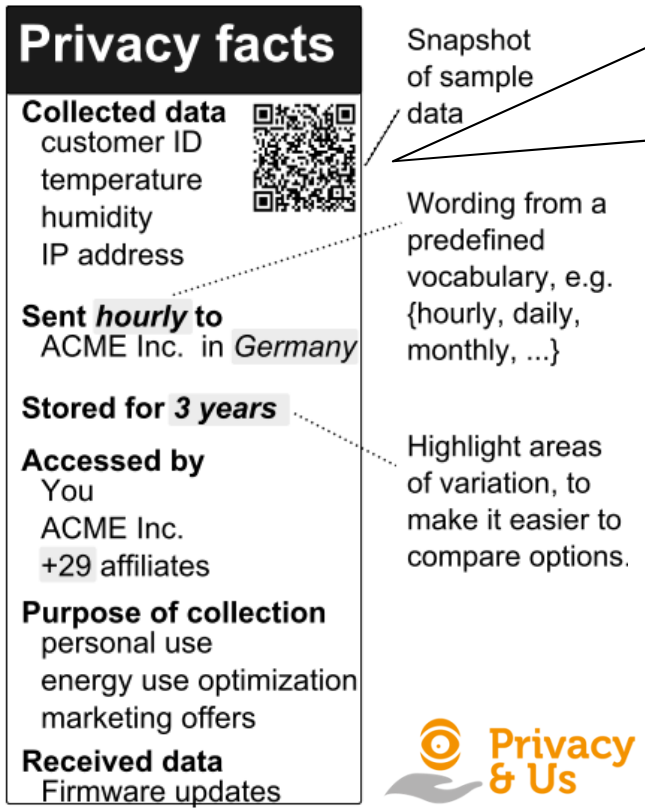
- Öffentliche Umgebung (z.B. Videoüberwachung) Schilder, Öffentlichkeitskampagnen, Ankündigung in den Medien, Markierungen auf dem Boden,...

- IoT, Devices ohne Bildschirm, Produktverpackungen: Icons, QR-Codes, Videos, SMS … Beispiel...

Praktische Hinweise

pre-acquisition → set up → use → maintenance → decommissioning

Kaufentscheidung => Setup => Nutzung => Wartung = > Entsorgung

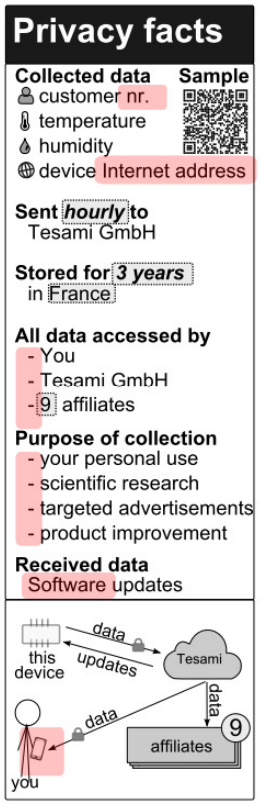


Text direkt im QR-Code:
customer number = 481-AHR-1831
temperature = 22 C
humidity = 34%
device Internet address = 93.184.216.34

Oder gleich der Link auf die passende (volle) Datensschutzerklärung https://www.datenschutzzentrum.de/datenschutzerklaerung/

Zur Veröffentlichung als D4.2 vorgesehen unter https://privacyus.eu/publications/deliverables/
Bis dahin: über LD610, LD6

Praktische Hinweise Laufende Arbeit...



Privacy & Us

Nur zum **INTERNEN GEBRAUCH** - laufende Arbeit von LD610
Bis dahin: über LD610, LD6

Praktische Hinweise

Gestern war Fließtext, morgen kommt SPECIAL –

Zukunftsmusik!

- Art. 21 (5) Widerspruch per automatisierter Verfahren unter Verwendung technischer Spezifikationen
- Art. 10 (1b) ePrivacy-VO (Parlamentsentwurf)
  Unbeschadet des Absatzes 1 kann, sofern der Datenschutzausschuss eine bestimmte Technologie zugelassen hat, für die Zwecke des Artikels 8 Absatz 1 Buchstabe b die Einwilligung jederzeit – sowohl in der Endeinrichtung als auch mittels von dem bestimmten Dienst der Informationsgesellschaft bereitgestellter Verfahren – erteilt oder widerrufen werden.

SPECIAL

Transparenz von Algorithmen

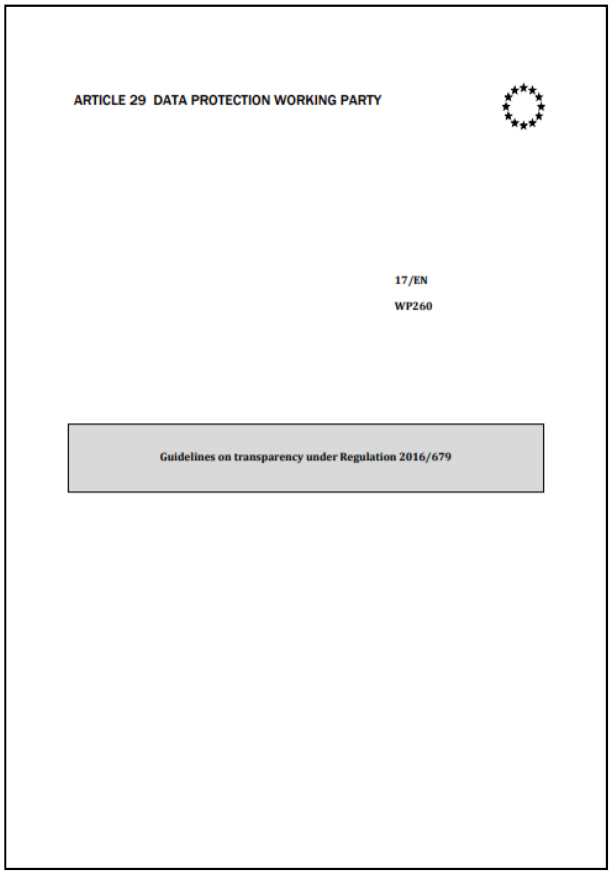
Zukunftsthema: Verständlichkeit von Algorithmen

Quellen zum Thema Transparenz und DSGVO

1. Verfassungsrang
   - Art. 8 EuGRCh – Fairnessprinzip

2. DSGVO
   - Art. 5 (1) (a)
   - Artt. 12 ff
   - Art. 15-22
   - Art. 34

3. Stellungnahmen:
   Art. 29 Datenschutzgruppe WP260
   (Bisher nur Englisch)


ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN
WP260

Guidelines on transparency under Regulation 2016/679

http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

Ausgewählte Fragestellungen aus dem Projektbereich des ULD

Schlüsselmanagement (VVV)

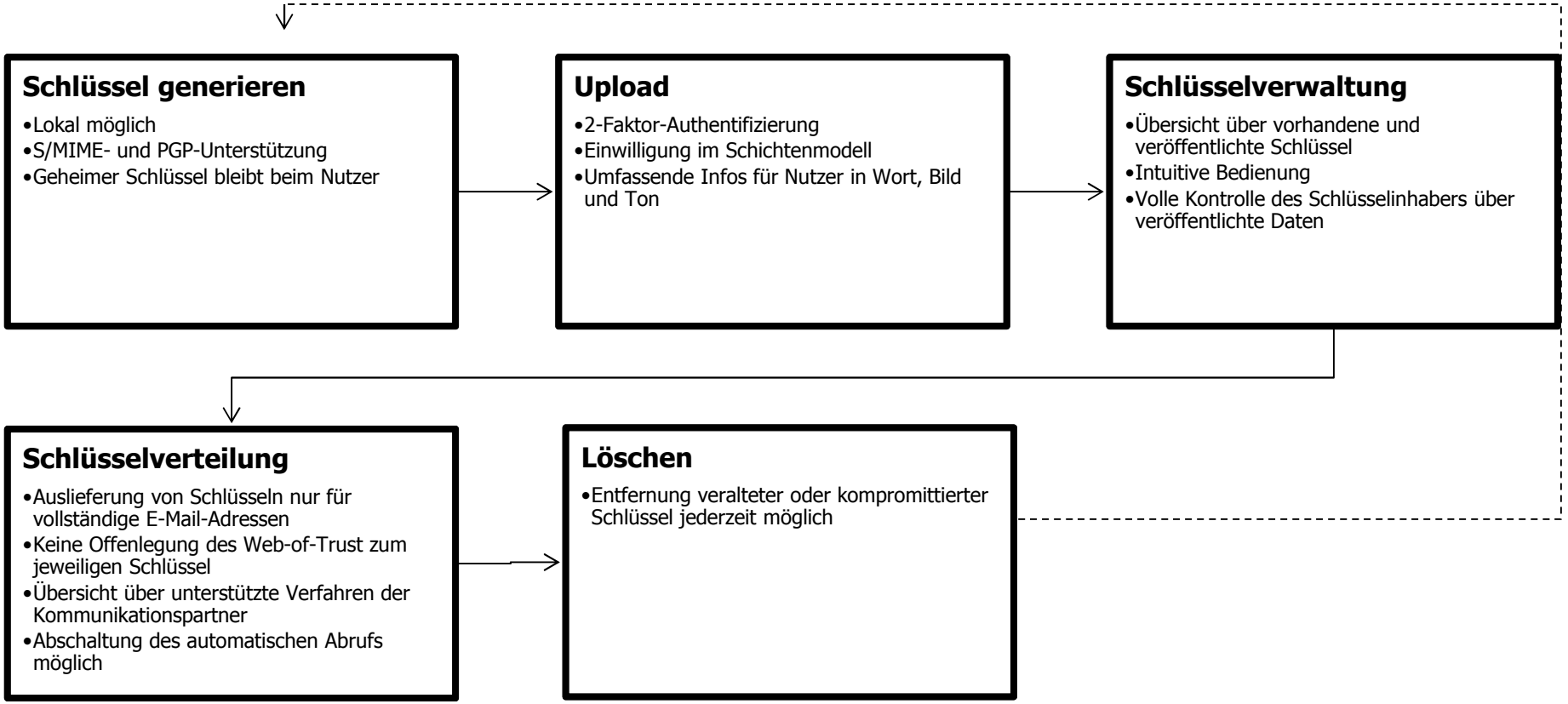
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Ende-zu-Ende-Verschlüsselung

- Ende-zu-Ende-Verschlüsselung von Kommunikation ist Idealzustand
- Problem ist die Verteilung öffentlicher Schlüssel:
  - PGP-Keyerver veröffenltichen mailadresse und „web of trust"
  - Auffinden der Schlüssel an zentraler Stelle (Keyserver) ist möglich aber aus datensparsamkeitsgründen unerwünscht
- Lösung: Bereitstellung beim Mailprovider des Empfängers
  - Mailprovder hat Vertrauen des Accountinhabers
  - Mailvprovider hat ohnehin Informationen über Kontakte

Data Protection by Design und Data Protection by Default

Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Unverkettbarkeit durch passgenaue Maßnahmen



ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Mehr unter: https://www.keys4all.de/

Herzlichen Dank für die gemeinsame Diskussion zum Thema

Kontakt:
Harald Zwingelberg
uld6@datenschutzzentrum.de
www.datenschutzzentrum.de
0431/988-1222

SPECIAL

Privacy & Us

SeDaFa
Selbstdatenschutz im vernetzten Fahrzeug

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein