Datenschutz – Chancen und kluge Nutzung digitaler Medien in der Selbsthilfe!

Marit Hansen, Christian Krause
Unabhängiges Landeszentrum für Datenschutz

Kiel, 24.10.2019

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

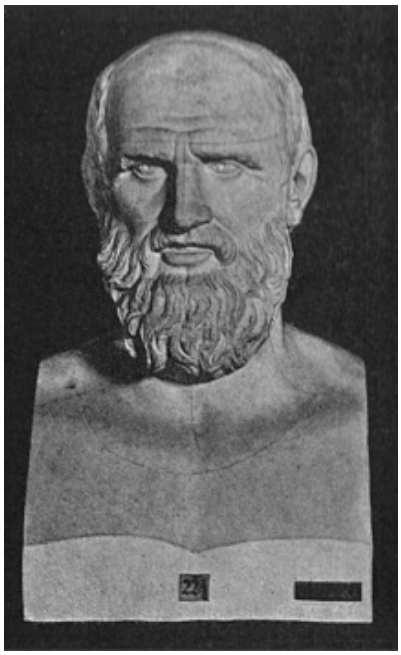
 Bild: kalhh via Pixabay

- Datenschutz und sensible Daten
- Verantwortung von Verarbeitern
- Nutzung digitaler Medien – was zu beachten?
- Fazit

Bild: Das Wortgewand via Pixabay

Datenschutz

- Nicht nur Sicherheit
- Faire Verarbeitung personenbezogener Daten



Vertraulichkeit bei medizinischer Behandlung

„Was ich bei der Behandlung
sehe oder höre oder auch
außerhalb der Behandlung
im Leben der Menschen,
werde ich, soweit man es nicht
ausplaudern darf, verschweigen
und solches als ein Geheimnis betrachten."

- Aus dem Hippokratischen Eid

Vertraulichkeit bei medizinischer Behandlung

§ 203 StGB – Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs [...]

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

[...]

Hier: für Heilberufler

Generell: Gesundheitsdaten sind sensibel!

Art. 9 Datenschutz-Grundverordnung:

- Alle Gesundheitsdaten sind sensibel
- Datenschutzrisiko berücksichtigen

Artikel 9

Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

Überblick

Bild: kalhh via Pixabay

- Datenschutz und sensible Daten
- Verantwortung von Verarbeitern
- Nutzung digitaler Medien – was zu beachten?
- Fazit

Verantwortung im Datenschutz

- Der Verantwortliche ist verantwortlich
  - Wer allein oder gemeinsam mit anderen „über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet"
  - Auch ein Verein
- Der Auftragsverarbeiter in seinem Bereich
- Ziel: Risikobeherrschung
- Nachweis der Datenschutzkonformität

- Ausnahme von Geltung der Datenschutzanforderungen: „natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten" („Haushaltsausnahme") [Art. 2 (2) c DSGVO]

Verantwortung im Datenschutz: Rechtsgrundlagen

Rechtsgrundlagen

- Einwilligung – freiwillig, informiert, widerrufbar [Art. 6 (1) a DSGVO]
- Vertrag [Art. 6 (1) b DSGVO]
- Erfüllung rechtlicher Verpflichtung [Art. 6 (1) c DSGVO]
- Erforderlichkeit für lebenswichtige Interessen [Art. 6 (1) d DSGVO]
- Aufgabe in Ausübung öffentlicher Gewalt [Art. 6 (1) e DSGVO]
- Berechtigte Interessen (in Abwägung mit den Rechten und Freiheiten der Betroffenen) [Art. 6 (1) f DSGVO]

https://www.datenschutzzentrum.de/praxisreihe/

Neu: Datenschutz „by Design" & „by Default"

- Anforderung nach Art. 25 DSGVO
- Pflicht für:
  - Datenverarbeiter (primär: Verantwortlicher)
  - Indirekt: Dienstleister und Hersteller von IT-Systemen
    - Aber: oft noch nicht die Regel
    - Nachfragen & einfordern
- Ziel: eingebauter Datenschutz von Anfang an
  a) datenminimierend
  b) mit möglichst datenschutzfreundlichen Voreinstellungen

Überblick

Bild: kalhh via Pixabay

- Datenschutz und sensible Daten
- Verantwortung von Verarbeitern
- Nutzung digitaler Medien – was zu beachten?
- Fazit

Verantwortung auch bei Einsatz von Technik

- Verwendung von Hard- und Software mit Daten über Menschen (z.B. Mitglieder) – Computer, Tablet, Smartphone, Telefon …
- Webseite
- E-Mail
- Soziale Medien wie soziale Netzwerke oder Messenger
- Datenspeicher auf Festplatte, USB-Stick oder in der Cloud

Pflichten:
- Festgelegte und dokumentierte Verarbeitung
- Meldungen bei Datenpannen [Art. 33 DSGVO]
- Auskunft, Korrektur, Löschung, …

Private Geräte im Einsatz

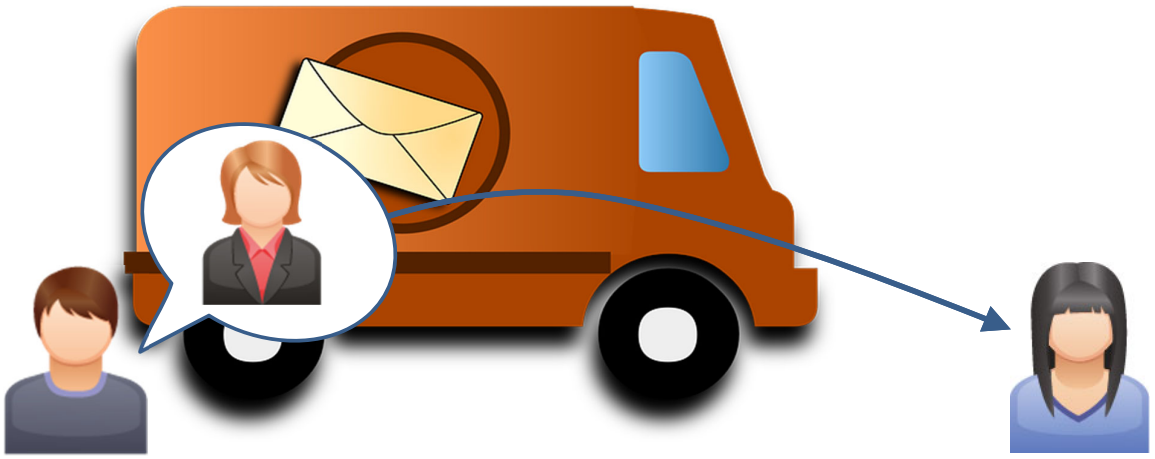
Bild: Clker-Free-Vector-Images via Pixabay

- BYOD – „Bring your own device“: problematisch
  - Verantwortung mit Rechenschaftspflicht
  - Mischung privat/nicht-privat
  - Sicherheit? Datenpannen?
  - Kontrollmöglichkeiten?
- Lösungen?
  - Getrennte Vereinsgeräte mit nötiger Funktionalität
  - Technische Sicherheitsgarantien

Bild: Gerd Altmann via Pixabay

Kommunikation…

- … beinhaltet Daten von **Sender** und **Empfänger**…
- … und bisweilen auch die Daten unbeteiligter **Dritter**…
- … und nutzt ein Medium (oder einen Dienstleister)



Risiken bei der Nutzung elektronischer Medien

- Datenverlust durch
  - Fahrlässigkeit
  - Diebstahl / Vandalismus
- Bruch der Vertraulichkeit und Integrität
- Kollaterale Verlaufs- und Metadaten
  - … in den Händen Dritter.

Fragen bei der Auswahl von Kommunikationsmedien

- Wer kontrolliert das Medium?
  Warum wird der Dienst angeboten?
  Wie wird er finanziert?
- Gibt es **Vertraulichkeit**?
  Liest jemand anderes mit?
- Gibt es **Integrität**?
  Kommt meine Nachricht unverändert an?
- Gibt es **Authentizität**?
  Ist die Identität des anderen gewiss?

Beispiel Dropbox

- Anbieter *Dropbox International Unlimited Company*, Irland
  Freemium-Geschäftsmodell
- Keine Verschlüsselung der Inhalte: Dropbox-Mitarbeiter haben theoretisch Zugriff
  → mäßige Vertraulichkeit
- Keine Sicherung der Integrität
- Zusammenarbeit über Links und ggf. Passwörter
  → ggf. ausreichende Authentizität

WhatsApp

- Anbieter *WhatsApp Ireland Limited*
  (Anschrift: 4 Grand Canal Square, Grand Canal Harbour, Dublin 2)
  Dienst gratis, Finanzierung über Datenweitergabe (auch von dritten), Datenauswertung und (demnächst) Werbeeinblendung
- Ende zu Ende-Verschlüsselung nach Stand der Technik
  → Vertraulichkeit gewährleistet
- Verschlüsselungsprotokoll verhindert unbefugte Änderungen
  → Integrität gewährleistet
- Empfänger wird nur anhand einer Telefonnummer identifiziert
  → schwache/fehleranfällige Authentizität

Facebook

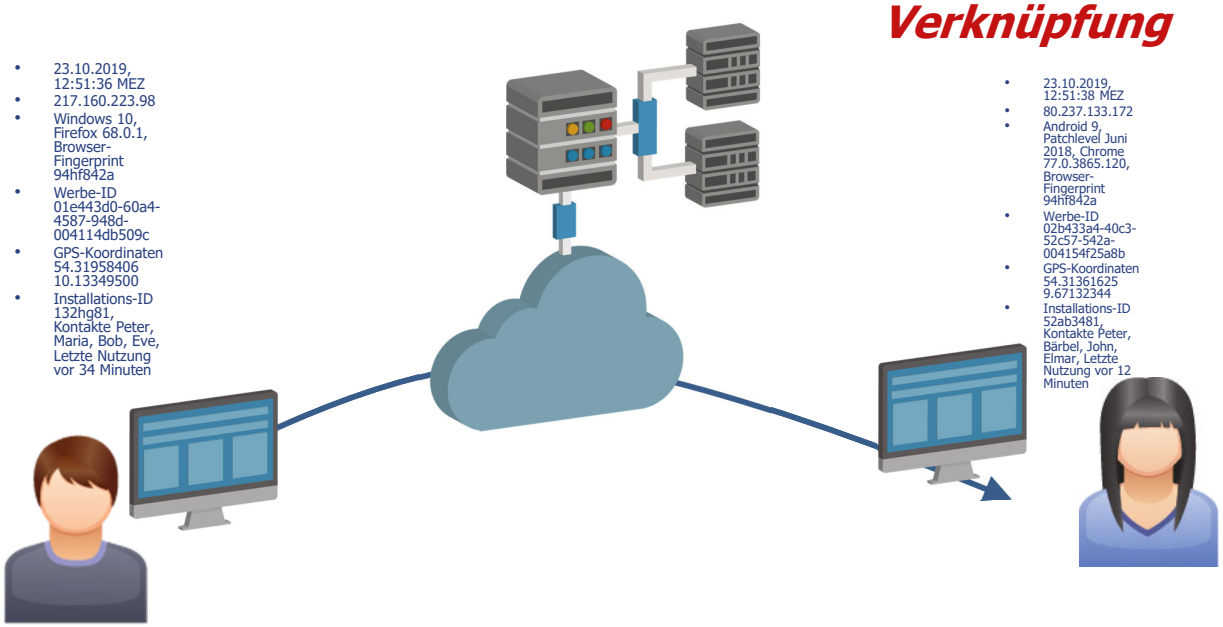
- *Anbieter:* Facebook Ireland Limited
  (Anschrift: 4 Grand Canal Square, Grand Canal Harbour, Dublin 2…)
  Gratis-Dienst, Finanzierung über Datenauswertung und Werbung
- Keine Verschlüsselung der Inhalte: Facebook-Mitarbeiter haben theoretisch Zugriff
  → mäßige Vertraulichkeit
- Keine Sicherung der Integrität
- Nutzerkonten sind frei erstellbar
  → geringe Authentizität

Verlaufs- und Metadaten

- Zeitstempel
- IP-Adresse
- Softwareparameter (Versionsnummern, verfügbare Programme, Schriftarten, Auflösung, Hardware-Eigenheiten)
- Werbe-ID
- GPS-Koordinaten
- Sonstige Sensordaten
- Aktivitätsdaten der konkreten Applikation (Verhaltensmuster, Kontakte)

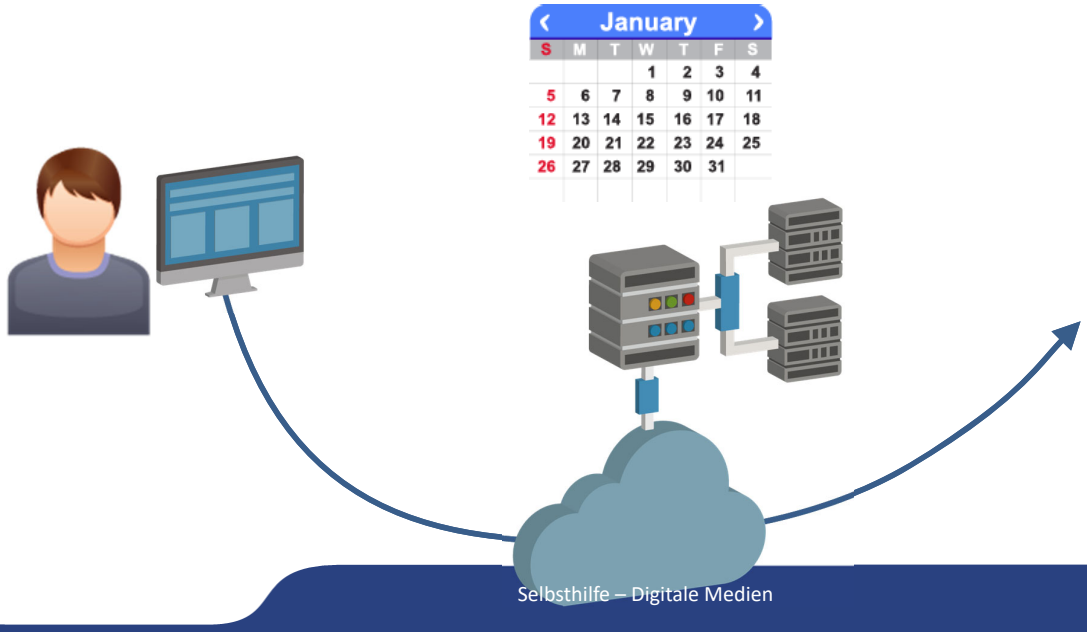
Verknüpfung

- 23.10.2019, 12:51:36 MEZ
- 217.160.223.98
- Windows 10, Firefox 68.0.1, Browser-Fingerprint 94hf842a
- Werbe-ID 01e443d0-60a4-4587-948d-004114db509c
- GPS-Koordinaten 54.31958406 10.13349500
- Installations-ID 132hg81, Kontakte Peter, Maria, Bob, Eve, Letzte Nutzung vor 34 Minuten



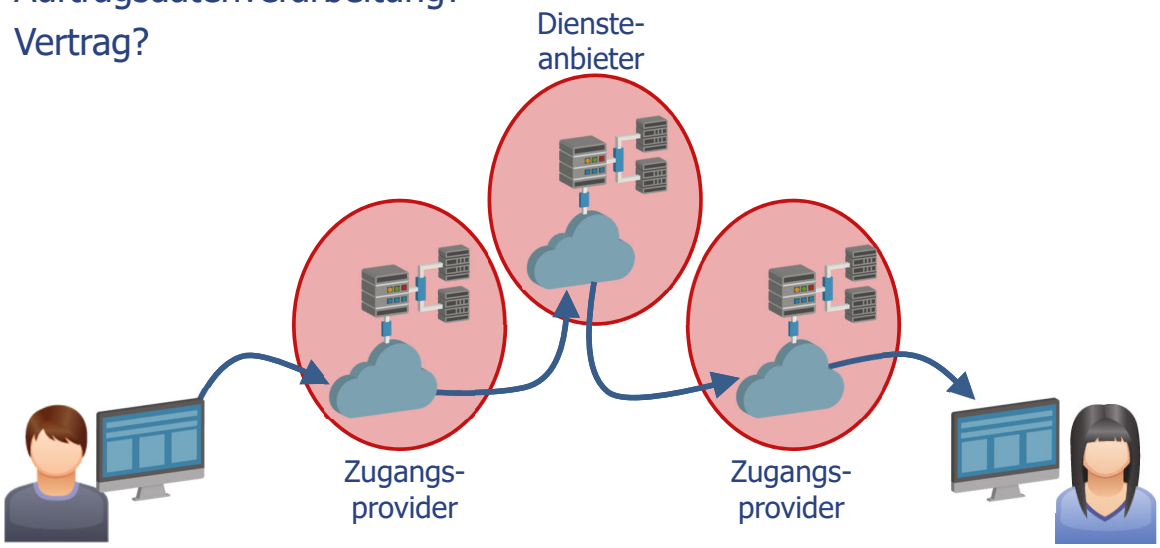
- 23.10.2019, 12:51:38 MEZ
- 80.237.133.172
- Android 9, Patchlevel Juni 2018, Chrome 77.0.3865.120, Browser-Fingerprint 94hf842a
- Werbe-ID 02b433a4-40c3-52c57-542a-004154f25a8b
- GPS-Koordinaten 54.31361625 9.67132344
- Installations-ID 52ab3481, Kontakte Peter, Bärbel, John, Elmar, Letzte Nutzung vor 12 Minuten

Verkettung



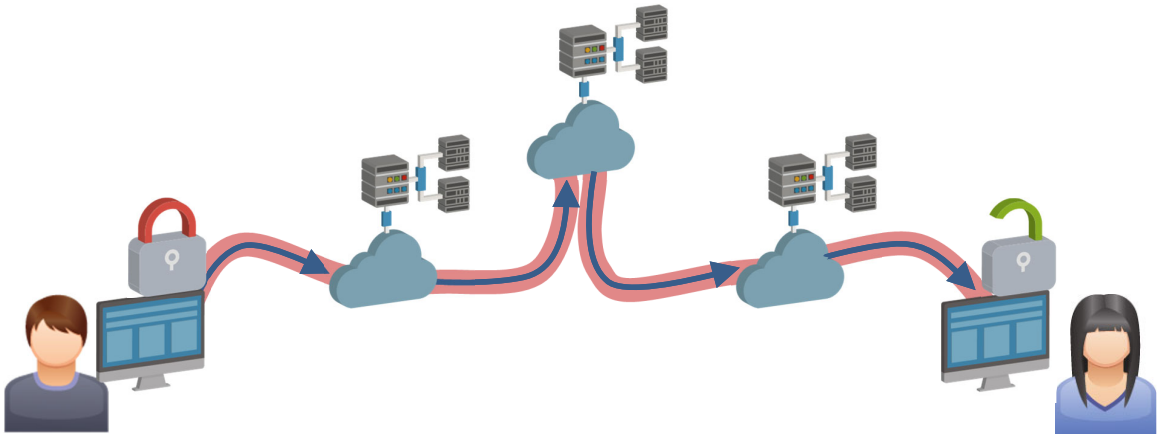
Auswahl der Dienstleister

- Auftragsdatenverarbeitung?
- Vertrag?



Informationen dem Dienstleister entziehen

- Ende-zu-Ende-Verschlüsselung
- Trotzdem fallen Meta-Daten an



Entscheidungen bei jedem Risiko

- Was soll geschützt werden? Schutzbedarf normal / hoch / sehr hoch
- Vor wem? Akteure Vor was? Eingriffe
- Welche Risiken bestehen? Ursachen, Auswirkungen, Wahrscheinlichkeiten
- Welche Schutzmaßnahmen sind möglich? Praktikabilität
- Welche Restrisiken verbleiben?

- Strategien zum Umgang mit Risiken:
  - Vermeiden
  - Reduzieren und begrenzen
  - (((Verlagern???)))
  - ~~Ignorieren~~

In jedem Fall:
sich informieren
(AGBs, Datenschutzerklärungen, Berichterstattung, …)

Gemeinsames Rundschreiben 2020

Beantragt eine Selbsthilfegruppe, Selbsthilfeorganisation oder Selbsthilfekontaktstelle Fördermittel nach § 20h SGB V verpflichtet sich der Antragsteller, die nachstehenden Grundsätze anzuerkennen und in der Praxis zu berücksichtigen.

1. Das Internetangebot bietet Transparenz
2. Informationen über Anbieter sind bereitgestellt
3. Einfache Kontaktaufnahme ist möglich
4. Nutzung ist nicht an Bedingungen geknüpft
5. Bereitgestellte Informationen und Hinweise sind nachvollziehbar
6. Datenschutzgesetze werden eingehalten
7. Technische Datensicherheit wird gewährleistet
8. Für Datensparsamkeit wird gesorgt
9. Keine Weitergabe personenbezogener Daten und Vermeidung von Tracking
10. Keine Nutzung sozialer Netzwerke für Austausch über Erkrankungen

Überblick

Bild: kalhh via Pixabay

- Datenschutz und sensible Daten
- Verantwortung von Verarbeitern
- Nutzung digitaler Medien – was zu beachten?
- Fazit

Datenschutz ist wie Hygiene

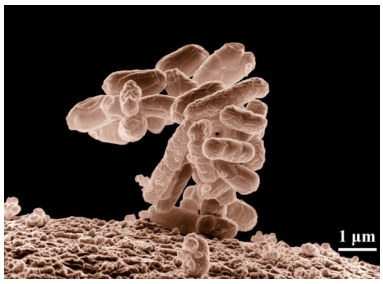


Bild: WikiImages via Pixabay

Bild: Jacqueline Macou via Pixabay

- Man kann die Bedrohungen oft nicht sehen. Oder zu spät.
- Späte Effekte möglich.
- Es betrifft einen selbst und andere. Jeder ist mitverantwortlich.

⇨Das richtige Verhalten sollte eingeübt und selbstverständlich sein.

Wichtig: alle mitnehmen

- Auch die, die nicht bei (allen) Sozialen Medien mitmachen
  - Weil sie nicht können
  - Weil sie nicht wollen
  - Weil es für sie riskant wäre
- Nicht Risiken für andere verursachen
  - Adressbuch!
  - Inhalte (z.B. Fotos)
  - Öffentliche Kommunikation nicht exklusiv auf 1 Kanal
- Aufklären, auch zu Selbstschutz

Datenschutz als Standard

- Bei Anbietern von Produkten oder Dienstleistungen Datenschutzgarantien nachfragen + einfordern
- Schulterschluss über Verbände in Deutschland oder Europa
- Beschwerdemöglichkeit bei Aufsichtsbehörden

Bild: Gerd Altmann via Pixabay

Fragen?

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein