Sommerakademie 2017

Infobörse 11

Neues aus der Datenschutzforschung –
Datenpannen, Transparenz, Dopingkontrolle

Susan Gonscherowski,
Torben Herber,
Harald Zwingelberg

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Datenpannen

Projekt EIDI: Effektive Information nach digitalem Identitätsdiebstahl

Susan Gonscherowski

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Die DSGVO und Datenpannen – was ist neu

- Art. 33 DSGVO Meldung an die Aufsichtsbehörde
  - Risikoanalyse statt allgemeiner Meldepflicht
  - Keine Einschränkung auf bestimmte Kategorien von Daten mehr
  - Adressat = Verantwortlicher iS des Art. 4 Nr.7

    sowohl öffentliche als auch nicht-öffentliche Stellen
  - Auftragsverarbeitern obliegt eine Meldepflicht ggü. Verantwortlichem

Die DSGVO und Datenpannen – was ist neu

- Art. 33 DSGVO Meldung an die Aufsichtsbehörde
  - One-Stop-Shop-Prinzip
  - Meldung an die Aufsichtsbehörde binnen 72h
  - Inhalt der Meldung:
    - Art der Verletzung, Art und Anzahl der Kategorien, ungefähre Zahl der Betroffenen und betroffenen Datensätze
    - Name und Kontaktdaten des DSB
    - Wahrscheinliche Folgen
    - Gegenmaßnahmen
  - Mögliche Bußgelder fallen deutlich höher aus

Die DSGVO und Datenpannen - was ist neu

- Art. 34 DSGVO Benachrichtigung des Betroffenen
  - Benachrichtigung als eigene Rechtsvorschrift
  - Hohes Risiko erfordert unverzügliche Benachrichtigung, außer:
    - Technische/organisatorische Sicherheitsvorkehrungen für betroffene Daten verhindern unbefugten Zugang/Zugriff
    - Das hohe Risiko wurde durch den Verantwortlichen bereits eliminiert
    - Unverhältnismäßig hoher Aufwand erfordert eine öffentliche Bekanntmachung oder vergleichbar wirkungsvolle Maßnahme
  - Klare, einfache Sprache
  - Aufsichtsbehörde kann Benachrichtigung der Betroffenen nachfordern oder per Beschluss den Verantwortlichen von der Pflicht entbinden

Schutzlücken

- Betroffene sind nicht immer bekannt, z.B. durch gezielte Angriffe auf ein bestimmtes Endgerät
- Die Benachrichtigung des Betroffenen hängt von der korrekten Risikoanalyse des Verantwortlichen ab
- Information der Öffentlichkeit durch Anzeigen erreicht wahrscheinlich nicht alle Betroffenen und enthält möglicherweise nicht alle für den Einzelfall relevanten Informationen
- Datenschutzvorfall und Identitätsdiebstahl können zeitlich sehr weit auseinander liegen und werden nicht in Verbindung gebracht

Projekt EIDI

- Betroffene werden gezielt und proaktiv informiert
- Für ältere Datenpannen erfolgt eine Risikoanalyse unter aktuellen Eintrittswahrscheinlichkeiten und Schadenshöhen
- Benachrichtigung kann unabhängig vom Verantwortlichen jederzeit nachgeholt werden
- Benachrichtigung enthält für den Betroffenen relevante Informationen

Ziele von EIDI

- Intervenierbarkeit für den Betroffenen verbessern
- Vertraulichkeit der personenbezogenen Daten wieder herstellen
- Integritätsverlusten vorbeugen
- Transparenz bei Datenschutzverletzungen erhöhen

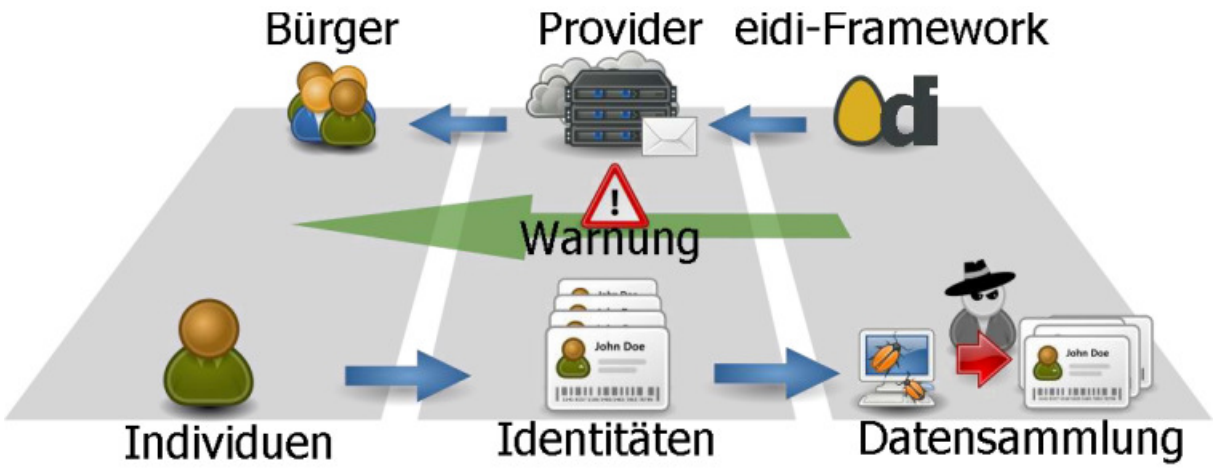

Abbildung 1: *Digitale Identitäten im Kontext von EI DI.*

Transparenz

Ergebnisse der Projekte
SPECIAL und iTESA

Harald Zwingelberg

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Gewährleistungsziel Transparenz

Transparenz bezeichnet die Anforderung, dass sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme hat.

Quelle: Standarddatenschutzmodell, S. 13.

Transparenz

- Transparenz ist ein zentrales Element der DSGVO.
- Bei Einwilligung ist Transparenz zwingender Bestandteil
- Bei gesetzlichen Tatbeständen muss die Transparenz proaktiv hergestellt werden, damit Betroffenenrechte nicht leer laufen (vergl. Art. 14 Erhebung nicht bei betr. Person).
- Detaillierte Information auf Anfrage durch den Betroffenen, Art. 15 DSGVO.

Transparenz bei bestehendem Kundenkontakt

- In der Regel eine Erhebung beim Betroffenen => Art. 13
  - Kundenkontakt, daher Einwilligung möglich
  - Widerruf einer Einwilligung ist zu beachten

- Bei Datenweitergabe an Dritte oder Zweckänderung durch Gewinnung neuer Informationen durch Analyse neue Einwilligung und Information erforderlich.

⇒ Einfache, vereinheitlichte Kommunikationsmöglichkeit mit Betroffenen wünschenswert

Transparenz bei öffentlich zugänglichen Daten

- Erhebung ohne Wissen der Betroffenen und ohne bestehenden Kundenkontakt,
  Beispiel Projekt iTESA mit Datenerhebung aus dem Netz

- Gesetzliche Rechtsgrundlage: Möglich hier Art. 6 (1) (f) DSGVO zur Wahrnehmung berechtigter Interessen des Verantwortlichen. Folgen:
  ⇒Art. 14 DSGVO Information des Betroffenen
  ⇒Art. 21 DSGVO Widerspruchsrecht

- Öffentliche Angaben z.B. auf der Webseite als Minimum notwendig, Art. 14 (5) (b) am Ende DSGVO.

Ausnahmen zugunsten von Big Data?

- Ausnahme des Art. 14 (5) (b) für Big Data?
  - Auskunftspflicht entfällt, sofern „sich die Erteilung […] als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde […]"
    Regelbeispiele dieser Ausnahme: insbesondere für öffentliche Archive, Forschungszwecke und Statistik.
  - Vorab: Entgegen reinem Gesetzestext ist eine **Abwägung** zwischen Aufwand für Verarbeiter und Interesse an der Information der betroffenen Person zwingend.
    [so zutreffend Kühling/Buchner/Bäcker Art. 14 DSGVO Rn. 55; schon zu Art. 11 DS-RiLi Dammann/Simitis Art. 11 RiLi Rn. 5]
  - Abwägungserfordernis folgt auch aus auch EU-weit allgemein gültigen Verhältnismäßigkeitsprinzip.

Ausnahmen zugunsten von Big Data?

- Ausnahme des Art. 14 (5) (b) für Big Data?
  - Wird Big Data per se bei vielen und nicht näher bekannten Betroffenen privilegiert?
  - Generelle Ausnahme für Big Data?

    ⇒Aber Abwägung zwingend (s.o.), keine generelle Lösung für Big Data

  - Gedanke des Art. 11 DSGVO keine Identifizierung allein zu Zwecken der DSGVO-Compliance, aber nach Erwägungsgrund 57 sind von Betroffenen beigebrachte Informationen zu Berücksichtigen

    ⇒ ergo: Prozess zur Unterrichtung Betroffener muss ohnehin etabliert sein

    ⇒ Berücksichtigung bei der Abwägung u.a. bei Quantifizierung des Risikos

Transparenz durch Data Protection by Design

- Ziele der Transparenz:
  - Verständlichkeit für Betroffene
  - Durchsetzbarkeit von Betroffenenrechten
  - Benennung von Akteuren (alle Verantwortliche, Auftragsverarbeiter)

- Umsetzung durch Tools möglich?

Beispiel
Widerruf per automatisiertem Verfahren

- Art. 21 (5) DSGVO ist Ausfluss des Privacy by Design (PbD)-Prinzips: [1]

  Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ungeachtet der Richtlinie 2002/58/EG ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.

- Widerspruch soll unkompliziert sein. Denkbar automatisierte Verfahren auf Basis lokal gesetzter Voreinstellungen.[2]

SPECIAL

[1] Paal/Pauly/Martini Art. 25 DSGVO Rn. 32.
[2] Paal/Pauly/Martini Art. 21 DSGVO Rn. 72.

Beispiel
Widerruf per automatisiertem Verfahren

- Umsetzung eines automatisierten Widerspruchs bedarf geeigneter Spezifikationen für die Kommunikation und eine geeignete Semantik zur Definition der Voreinstellungen „Privacy Preferences".

- Hier sollte auf bestehende Ergebnisse aus der Datenschutz-Forschung aufgebaut werden (P3P, PrimeLife Policy Language)

- Das Projekt „Scalable Policy-awarE linked data arChitecture for prIvacy, trAnsparency and compliance" (SPECIAL) nimmt sich Teilen dieser Aufgabe im Themenkreis Big Data an. Wunsch: W3C-Spezifikation Partner u.a. W3C (ERCIM), WU Wien, ULD und Unternehmen.

- Ziel: Erstellen einer Spezifikation, ggf. auch für Einwilligungen.
- https://www.specialprivacy.eu/

SPECIAL

Transparenz und das Internet of Things Herausforderungen

- Datenschutz im IoT-Produktzyklus und Wunschvorstellungen
  - Vor dem Kauf: Werbung, Verkaufsverpackung informiert (z.B. DV in Drittstaat), weitere Produktinformationen
  - Inbetriebnahme: Konfiguration, Voreinstellungen, Einbindung in eigene Infrastruktur vs. Cloud
  - Betrieb: Eingriffsmöglichkeiten, klare Datenflüsse, Erkennbarkeit für Dritte & Besucher
    (P) Systeme ohne Bedienelemente => Smartphone?
  - Wartung: Sicherheitsupdates
  - Außerbetriebnahme: Löschen, Entsorgung,

Privacy & Us

Herausforderungen Internet of Things IoT

- Wünsche an IoT aus Nutzerumfrage:
  - Einfache Nutzbarkeit
  - Kompatibilität mit vorhandenen Devices
  - Preis
  - …
- Frage: Brauchen IoT-Devices Updates?
  - 92% ja
- Wer ist verantwortlich, Updates einzuspielen?
  - Hersteller: 60 %
  - Eigentümer: 44 %
- These: „Nutzer sehen IoT-Devices als Gadgets nicht als Computer“ wurde in Umfrage falsifiziert,
  aber 55% IT-affine Teilnehmer / Experten

Privacy & Us

Datenschutz und Dopingkontrollen

PARADISE

Privacy-enhancing And Reliable Anti-Doping Integrated Service Environment

Torben Herber

Bundesministerium
für Bildung
und Forschung

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Das Anti-Doping Kontrollsystem

Bild: Jörg Daling

- Fokussierung auf *Whereabouts* (Ortsangaben)
- ca. *2.500* Athletinnen und Athleten in DEU betroffen
- **ADAMS** =
  Anti-**D**oping **A**dministration and **M**anagement **S**ystem
- Online Kalender
- quartalsweise *Eintragungs-* sowie *Aktualisierungspflichten* aufgrund des *Nationalen Anti-Doping Code* (NADC)
- Sanktionen (Sperren) bei Verstößen
- notwendig für die Planung & Durchführung *effektiver* Dopingkontrollen
- Kritik: Starker Eingriff in das Allgemeine Persönlichkeitsrecht der Athletinnen und Athleten

Das Projekt PARADISE

- zweijähriges Forschungsprojekt
- **Ziel:** *effektive* und *datenschutz-konforme* Anti-Doping Kontrollen
- **Lösungsansätze:**
  - Einsatz von *Eves Devices* (GPS)
  - vergröberte Positionsangaben für die Kontrollplanung
  - *zweckgebundener* Datenzugriff
  - *Logging* von Zugriffen
  - nachträgliche *Einseh- und Kontrollmöglichkeiten*
  - Einsatz von *Geofences*
  - *Sealed Cloud* Implementierung

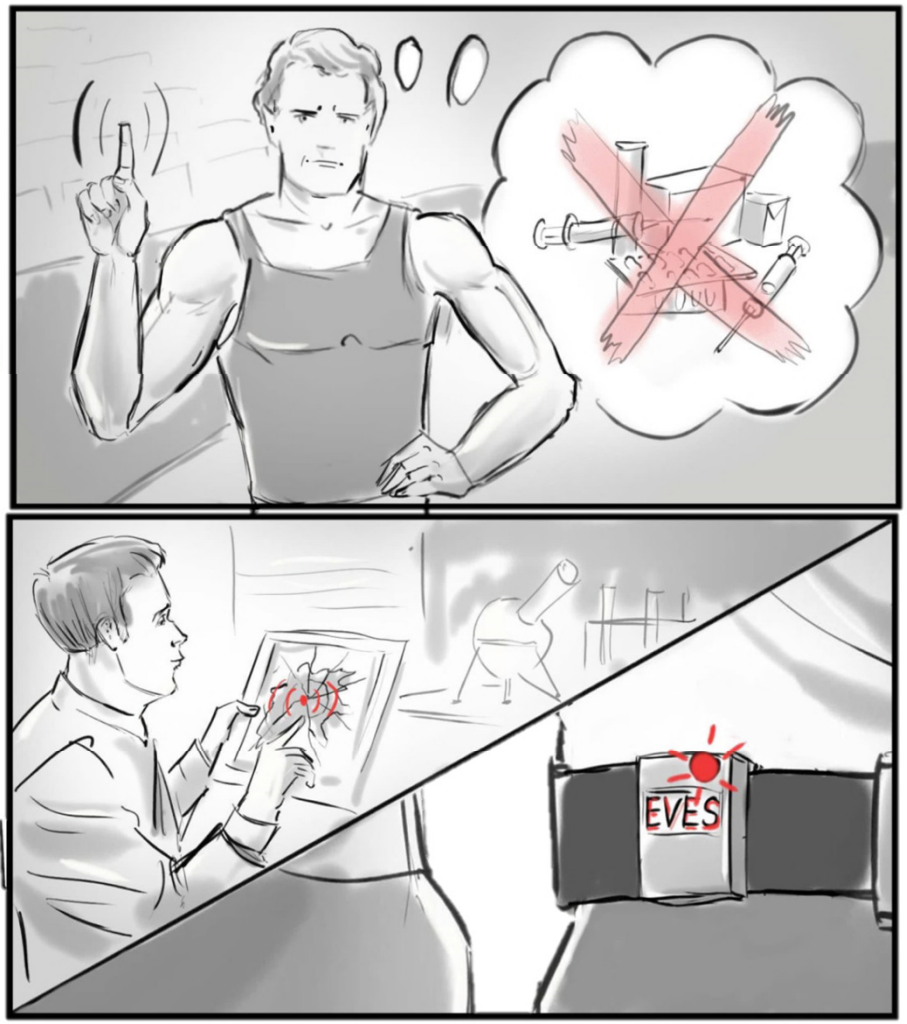

Bild: Jörg Daling

Bild: Jörg Daling

PARADISE *Veröffentlichungen*

Weiterführende Informationen zum Projekt PARADISE:

- Projektwebsite: www.privacy-paradise.de
- Datenschutz und Dopingkontrollen, DuD 7/2017, S. 427-433.
- ARD Sportschaubeitrag vom 25.02.2017 (abrufbar bis zum 25.02.2018) : http://www.sportschau.de/doping/gps-ueberwachung-fuer-dopingkontrollen-100.html
- Deutschlandfunk Beitrag, Online, 26.02.2017: http://www.deutschlandfunk.de/dopingpraevention-gps-sender-totale-ueberwachung-oder.1346.de.html?dram:article_id=379927
- Sportler wollen sich nicht mehr nackig machen, Zeit Online, 07. Dezember 2016: http://www.zeit.de/sport/2016-11/doping-datenbank-alternative-jonas-plass/komplettansicht

Förderhinweis

PARADISE
Privacy-enhancing And Reliable Anti-Doping Integrated Service Environment

Privacy-enhancing And Reliable Anti-doping Integrated Service Environment (PARADISE)

intelligent Traveller Early Situation Awareness (iTESA)

SPECIAL

Scalable Policy-awarE linked data arChitecture for prIvacy, trAnsparency and compliance (SPECIAL)

Effektive Information nach digitalem Identitätsdiebstahl (EIDI)

Projekte gefördert vom Bundesministerium für Bildung und Forschung:

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Gefördert durch die Europäische Kommission im H2020 Rahmenprogrammn unter Grant Agreeement 731601

Links: https://www.datenschutzzentrum.de/projekte/

Vielen Dank für Ihre Aufmerksamkeit

Kontakt:
Susan Gonscherowski
uld611@datenschutzzentrum.de
Torben Herber
uld612@datenschutzzentrum.de
Harald Zwingelberg
uld6@datenschutzzentrum.de
www.datenschutzzentrum.de
0431/988-1222

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein