Die EU-Datenschutz-Grundverordnung

Folgerungen für Deutschland, DESY und jeden Einzelnen

Carsten Porthun
Zeuthen, 12.06.2018

HELMHOLTZ SPITZENFORSCHUNG FÜR GROSSE HERAUSFORDERUNGEN

DESY.


Mostly blocked by idiots
@FeeMitV2EH
#DSGVO ist, wenn Du plötzlich ohne eigenes Zutun aus sämtlichen Newsletter fliegst, was Dir vorher trotz eigenem Zutun nicht gelungen ist.

EU Grundrechte-Charta

Datenschutz als Grundrecht

- **Artikel 1 - Würde des Menschen:**

  Die Würde des Menschen ist unantastbar. Sie ist zu achten und zu schützen.

- **Artikel 8 - Schutz personenbezogener Daten:**

  *(1) Jede Person hat das **Recht auf Schutz** der sie betreffenden **personenbezogenen Daten**.*

  *(2) Diese Daten dürfen nur nach **Treu und Glauben** für **festgelegte Zwecke** und mit **Einwilligung** der betroffenen Person oder auf einer sonstigen **gesetzlich geregelten legitimen Grundlage** verarbeitet werden. Jede Person hat das Recht, **Auskunft** über die sie betreffenden erhobenen Daten zu erhalten und die **Berichtigung** der Daten zu erwirken.*

  *(3) Die Einhaltung dieser Vorschriften wird von einer **unabhängigen Stelle** überwacht.*

Quelle: http://www.europarl.europa.eu/germany/de/die-eu-und-ihre-stimme/grundrechtecharta

Artikel 4

Personenbezogene Daten

„… alle Informationen, die sich auf eine **identifizierte** oder **identifizierbare natürliche Person** (im Folgenden „betroffene Person“) beziehen;

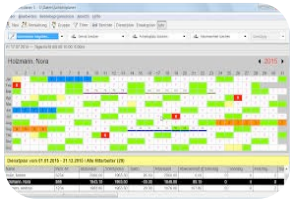
als identifizierbar wird eine **natürliche Person** angesehen, die direkt oder indirekt, insbesondere **mittels Zuordnung**

zu einer **Kennung** wie einem Namen,
zu einer **Kennnummer**,
zu **Standortdaten**,
zu einer **Online-Kennung** oder
zu einem oder mehreren **besonderen Merkmalen identifiziert werden** kann, die Ausdruck der
physischen,
physiologischen,
genetischen,
psychischen,
wirtschaftlichen,
kulturellen oder
sozialen Identität
dieser **natürlichen Person** sind.“

Beispiele für Verarbeitungen von pbD

Personaldaten

Betrieb von IT-Systemen



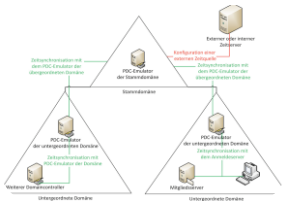
Schichtplanung

Webserver

Netzwerk-infrastruktur

Telefonanlage

Housing



Domänenbetrieb

Konferenzen

Warenwirtschaft

Printing

Userverwaltung

Guest-Net-Portal

Ticketsystem

Gruppenwebseiten

Artikel 5

Grundsätze für die Verarbeitung personenbezogener Daten

- Rechtmäßigkeit, Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Nachweispflicht der Einhaltung der Grundsätze

Artikel 6

Rechtmäßigkeit der Verarbeitung

Alles ist verboten, es sei denn:

- **Qualifizierte Einwilligung**
- Zur **Vertragserfüllung mit einer betroffenen Person**, oder zur Durchführung von **vorvertraglicher Maßnahmen**, die im Auftrag der betroffenen Person erfolgen
- Zur **Erfüllung einer rechtlichen Verpflichtung**, der betroffene Person unterliegt, erforderlich
- Zum **Schutz lebenswichtiger Interessen** der betroffenen Person oder anderer natürlicher Personen
- Im **öffentlichen Interesse** oder zu **Wahrung hoheitlicher Aufgaben**
- Zur Wahrung **berechtigter Interessen des Verantwortlichen** oder eines Dritten, wenn Interessen, Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen

Was hat sich geändert?

- Verknüpfung zu IT-Sicherheit
  - Risikobewertung nach PDAC Prinzip
  - Stand der Technik
- Privacy by Default / Privacy by Design
- Datenschutzfolgeabschätzung

- Informationspflichten
- Meldung von Datenschutzverstößen

- Marktortprinzip, One-Stop-Shop und Kohärenzverfahren

- Sanktionen:
  - BDSG : 50.000€ / 300.000 €
  - DSGVO: bis zu 4% weltweiter Jahresumsatz bzw. 20 Mio €

Artikel 32

Sicherheit der Verarbeitung

- Auswahl geeigneter technischer und organisatorischer Maßnahmen unter Berücksichtigung

Stands der Technik

Implementierungs-kosten

Art, Umfang, Umstände und Zweck der Verarbeitung

Eintrittswahrschein-lichkeiten und Schwere von Risiken für Rechte und Freiheiten

- Einzuschließen ist:
  - Pseudonymisierung und Verschlüsselung von pbD
  - Fähigkeit Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste auf Dauer sicher zu stellen
  - Fähigkeit Verfügbarkeit von pbD nach Zwischenfällen schnell wieder sicher zu stellen
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs zur Gewährleistung der Sicherheit der Verarbeitung

Änderungen bei den Betroffenenrechten

Recht auf Transparenz / Information

Auskunftsrecht

Recht auf Berichtigung

Recht auf Löschung

Recht auf Einschränkung der Verarbeitung

Recht auf Datenübertragbarkeit

Widerspruchsrecht

Was ist zu tun?

Prozessverantwortlich?	• Datenschutzbeauftragten kontaktieren • Aktualisierung der Prozessdokumentation • Technik / Organisation anpassen (Art. 32)
Dienstleister im Einsatz?	• Anpassung der Verträge (Art. 28)
Einwilligung als Grundlage?	• Einwilligung anpassen (Art. 12) • Einwilligung einholen

Artikel 30

Prozessdokumentation

- Rechtsgrundlage und Zweck
- Kategorien betroffener Personen
- Kategorien von personenbezogenen Daten
- Schnittstellen zu anderen Verfahren / Prozessen
- Kategorien von Empfängern
- Speicherdauer
- Eingesetzte Tools
- Erforderliches Maß an Vertraulichkeit, Integrität und Verfügbar
- Technische und organisatorische Maßnahmen

Probleme

- Welche Rechtsgrundlage ist anwendbar?
  - DSGVO, BDSG neu, TKG, TMG, KuhG, ….?
  - ePrivacy-Verordnung – wann kommt sie?
  - Landes-Datenschutzgesetze?

- Bislang keine Rechtssprechung

- Fokus der Gesetzgebung
  - BDSG: die Erhebung
  - DSGVO: die Verarbeitung

Fragen?

Carsten Porthun

040 / 8998 2553

carsten.porthun@desy.de

datenschutz@desy.de

https://datenschutz.desy.de