Datenschutz und Asylhilfe

23. Oktober 2018

eureos

I. DS-GVO

eureos

Gliederung

- Anlass DS-GVO
- Überblick neue gesetzliche Regelungen
- Eckpunkte

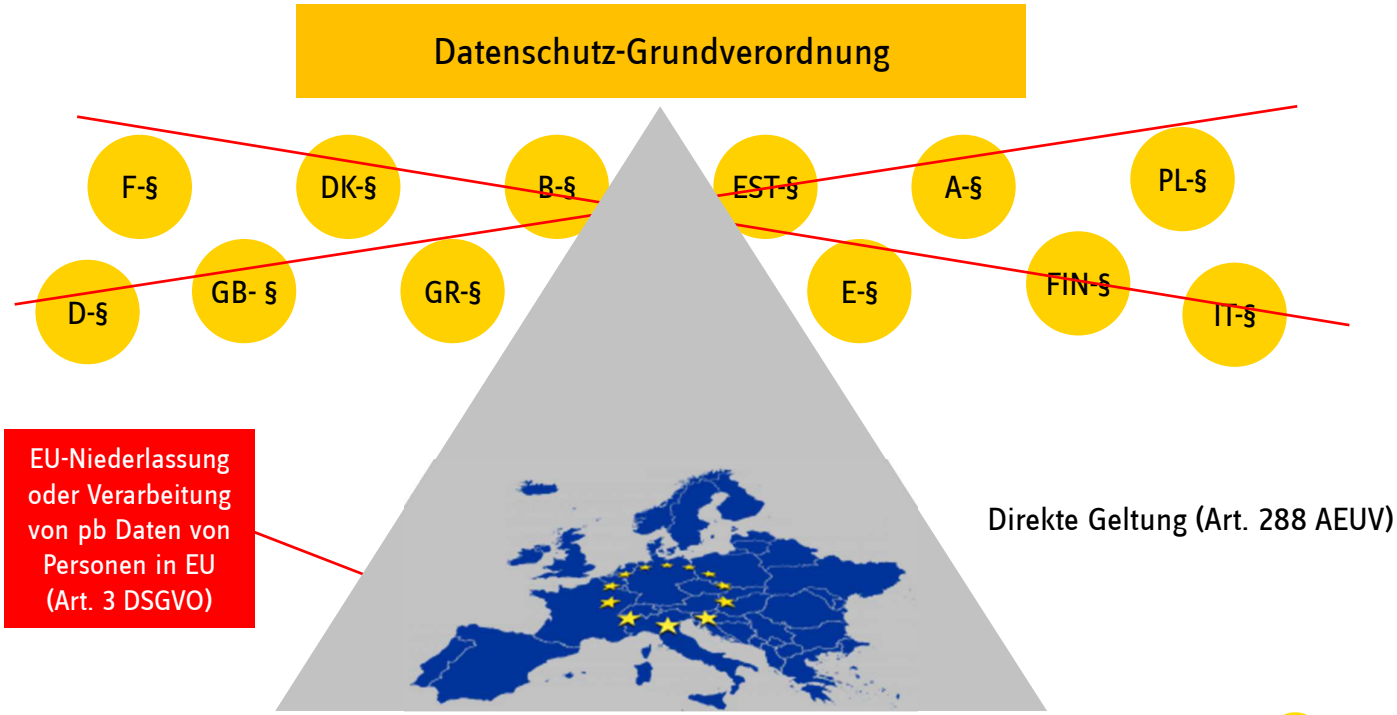
Anlass

Schutz personenbezogener Daten

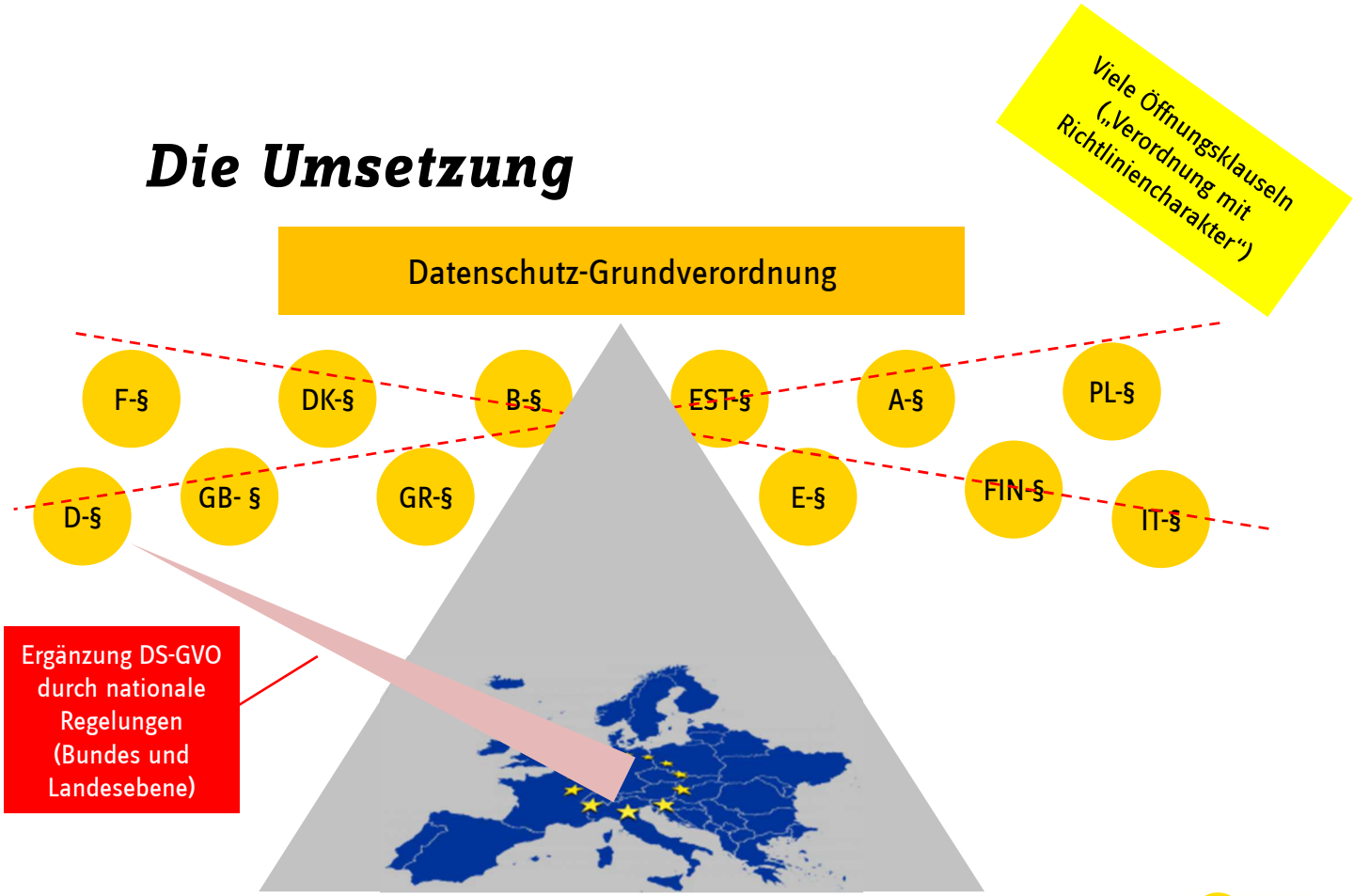
Rechtslage alt

Office of the Data Protection Commissioner. Canal House, Station Road, Portarlington, Co. Laois, Ireland.

Der Plan



Die Umsetzung



DS-GVO

Viele formelle Änderungen, wenige materielle

- Deutliche Ausweitung der **Dokumentationspflichten** (vgl. Art. 5 Abs. 2 DS-GVO)
- Deutliche Ausweitung der **Betroffenenrechte** (inkl. Festlegung von Fristen, vgl. Art. 12-23 DS-GVO)
- Deutliche Ausweitung der **Bußgeldtatbestände und -höhen** (aber schon unter BDSG a.F. war Gewinnabschöpfung möglich)
- Risikobeurteilungen und **Folgenabschätzung** (in weiterem Umfang als bisherige Vorabkontrolle)
- **Privacy by design** und **Privacy by default** werden verbindlich
- Mehr Pflichten und größere Haftungsrisiken für **Auftragsverarbeiter**
- **Wenige materielle Änderungen** (d.h. Rechtmäßigkeit Umgang mit pbD)

Überblick

Neue gesetzliche Regelungen

Überblick

	DV öffentliche Hand + Privatw.	Polizeiliche Zusammenarbeit	Online-Kommunikation	Andere Nicht-EU DV
EU	Datenschutz-Grund-verordnung =DS-GVO (2016/679; ab 25.5.2018)	Datenschutz RL Justiz und Inneres = JI-RL (2016/680/EG)	ePrivacy VO (Entwurf) ab 25.5.2018	
	Öffngs kl / Schran ken			
Bund	BDSG neu, Teil I + II (ab 25.5.2018)	BDSG neu, Teil I + III	TMG neu TKG neu § 7 UWG Änderungen	BDSG neu, Teil I + IV
Land	ThürDSG ab 25.5.2018			

Praktische Handhabung Gesetze

Paralleles Lesen von DS-GVO und BDSG bzw. ThürDSG

DATAKONTEXT

Datenschutz-Grundverordnung - BDSG

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

Inhalt:

KAPITEL I	Allgemeine Bestimmungen
Artikel 1	Gegenstand und Ziele
Artikel 2	Sachlicher Anwendungsbereich
§ 1 BDSG	Anwendungsbereich des Gesetzes
Artikel 3	Räumlicher Anwendungsbereich
Artikel 4	Begriffsbestimmungen
§ 2 BDSG	Begriffsbestimmungen
KAPITEL II	Grundsätze
Artikel 5	Grundsätze für die Verarbeitung personenbezogener Daten
Artikel 6	Rechtmäßigkeit der Verarbeitung
§ 3 BDSG	Verarbeitung personenbezogener Daten durch öffentliche Stellen
§ 4 BDSG	Videoüberwachung öffentlich zugänglicher Räume
§ 23 BDSG	Verarbeitung zu anderen Zwecken durch öffentliche Stellen
§ 24 BDSG	Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen
§ 25 BDSG	Datenübermittlungen durch öffentliche Stellen
§ 26 BDSG	Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses
Artikel 7	Bedingungen für die Einwilligung
Artikel 8	Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informations-gesellschaft
Artikel 9	Verarbeitung besonderer Kategorien personenbezogener Daten
§ 22 BDSG	Verarbeitung besonderer Kategorien personenbezogener Daten
§ 24 BDSG	Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen

https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_6.pdf

Praktische Handhabung Gesetze

Erwägungsgründe mitlesen

DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO) | ERWÄGUNGSGRÜNDE | BDSG (NEU) | English

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
61	62	63	64	65	66
67	68	69	70	71	72
73	74	75	76	77	78
79	80	81	82	83	84
85	86	87	88	89	90
91	92	93	94	95	96
97	98	99	100	101	102
103	104	105	106	107	108
109	110	111	112	113	114

Erwägungsgrund 39

Grundsätze der Datenverarbeitung*

[1] Jede Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen. [2] Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. [3] Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. [4] Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden. [5] Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im

www. https://dsgvo-gesetz.de

Eckpunkte

Eckpunkte

- Sachlicher Anwendungsbereich (Art. 2)
- Persönlicher Anwendungsbereich (Art. 4 Nr. 7, 8; Art. 24 ff.)
- Territorialer Anwendungsbereich (Art. 3)
- Grundprinzip für normale personenbezogenen Daten (Art. 6)
- Grundprinzip für besondere personenbezogenen Daten (Art. 9, 10)
- Grundsätze (Art. 5)
- Pflichten VA / Betroffenenrechte (Art. 12 – 22)
- Datenschutzerklärung Website

- Auftragsverarbeiter (Art. 28)
- Datenschutz-Folgenabschätzung (Art. 35)
- Datenschutzbeauftragter (Art. 37-39)
- Verpflichtung auf das Datengeheimnis
- Trans Border Data Flow (Art. 44-50)
- Arbeitsrecht (Art. 88)
- Datensicherheit
- Data protection by design / Data protection by default
- Meldepflichten
- Geldbußen (Art. 83)
- Sanktionen (Art. 84)

Sachlicher Anwendungsbereich

Rechtsgrundlage

Artikel 2
Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die ganz oder teilweise **automatisierte Verarbeitung personenbezogener Daten** sowie für die **nichtautomatisierte** Verarbeitung personenbezogener Daten, die in einem **Dateisystem** gespeichert sind oder gespeichert werden sollen....

Sachlicher Anwendungsbereich

Inhalt

- **personenbezogene Daten**
- **Verarbeitung**
  - automatisiert (Regel) oder
  - (manuell) von pbD, die in einem Dateisystem gespeichert sind oder gespeichert werden
- **Nicht: Außerhalb des Anwendungsbereichs des Unionsrechts (Art. 2 Abs. 2 Buchstabe a DSGVO)**
  - Nationale Sicherheit (Verfassungsschutzbehörden etc.)
  - Parlamentarische Tätigkeit des Landes etc.

Sachlicher Anwendungsbereich

Personenbezogene Daten

- **Definition Art. 4 Nr. 1**

> „...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;"

- **nur Daten von natürlichen Personen (vgl. aber BGH, BVerfG: Auch juristische Personen haben Recht auf informationelle Selbstbestimmung)**
- **nur von lebenden Personen (Erwägungsgrund 27; vgl. aber BGH, Urt. v. 1.12.1999 - I ZR 49/97 - Marlene Dietrich zum postmortalen Persönlichkeitsrecht)**
- **identifiziert oder identifizierbar (dazu Erwägungsgrund 26, 30)**

Sachlicher Anwendungsbereich

Personenbezogene Daten

- **Anonymisieren**

> „... ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können" (§ 3 Abs. 6 BDSG a.F.)

  - U.U. keine personenbezogenen Daten mehr (vgl. EG 26 Satz 5 und 6)
  - Problem: De-Anonymisierung durch Big Data möglich

- **Pseudonymisieren**

> „... „ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren" (§ 3 Abs. 6a BDSG a.F.)

  - = personenbezogene Daten!
  - Verschlüsselung = pseudonymisierte Daten

Sachlicher Anwendungsbereich

Verarbeiten

- Weiter Begriff
- Jeder … Vorgang … im Zusammenhang mit personenbezogenen Daten.
- Erheben, Speichern, Ändern, Nutzen, Übermitteln, Löschen, incl. Profiling und Scoring
- Art. 4 Abs. 2

Persönlicher Anwendungsbereich

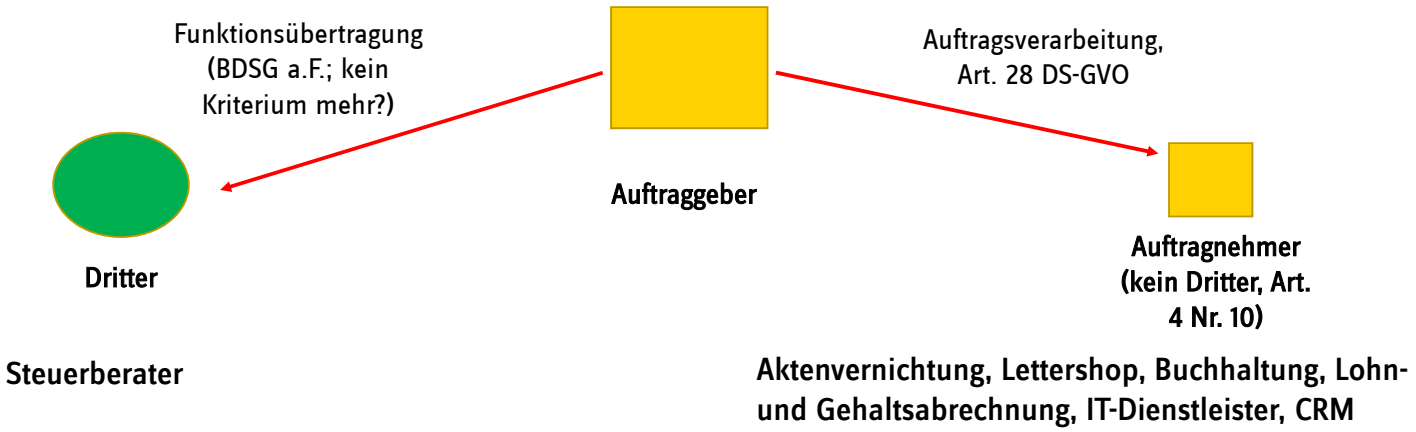
1. Verantwortlicher

Art. 4 Nr. 7: Jeder, der personenbezogene Daten verarbeitet.

- Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,
- die allein oder gemeinsam mit anderen
- über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet

Persönlicher Anwendungsbereich

2. Auftragsverarbeiter (neu)



Steuerberater

Aktenvernichtung, Lettershop, Buchhaltung, Lohn- und Gehaltsabrechnung, IT-Dienstleister, CRM

➢Mehr unmittelbare gesetzliche Pflichten (Meldepflichten für „data breach", Bestellung DSB, Verfahrensverzeichnis, Schadensersatz, Benennung EU-Vertreter)

Grundprinzip normale pbD

Inhalt

- **<u>Verbot mit Erlaubnisvorbehalt</u> (ähnlich BDSG)**
- **Kein Anwendungsvorrang: Alle Rechtfertigungsgründe stehen nebeneinander**
- **Große Änderung gegenüber bisheriger Praxis erwartet (Hoeren; a.A. Düsseldorfer Kreis)**
- Gilt für alle personenbezogenen Daten, die <u>nicht</u> zu Kategorie der besonderen Daten nach Art. 9 oder zu Art. 10 zählen
- Buchstabe e: Zentraler Erlaubnistatbestand für öffentliche Stellen
- Öffnungsklauseln betr. Buchstaben c + e (Art. 6 Abs. 2, Abs. 3)

Grundprinzip normale pbD

Rechtsgrundlage

	Art. 6 Abs. 1 lit. a DSGVO	Einwilligung („unmißverstdl.“)	
Ge-setz	Art. 6 Abs. 1 lit. b DSGVO	Vertragsdurchführung	
	Art. 6 Abs. 1 lit. c DSGVO	Rechtliche Verpflichtungen	+ BDSG
	Art. 6 Abs. 1 lit. d DSGVO	Lebenswichtige Interessen	
	Art. 6 Abs. 1 lit. e DSGVO	Öffentliches Interesse	+ BDSG
	Art. 6 Abs. 1 lit. f DSGVO	Interessensabwägung	

Grundprinzip normale pbD

Einwilligung (lit. a)

- **Legaldefinition:**

  „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;“ (Art. 4 Nr. 11)
- **ausreichend: „unmissverständlich“ („unambiguous“); anders Art. 9 Abs. 2 (s.u.)**
- **Darlegungslast bei Verantwortlichem (Art. 7 Abs. 1)**
- **In AGB: getrennt, deutlich lesbar, einfach zugreifbar (Art. 7 Abs. 2)**
- **Einwilligung von Kindern (Art. 8): Erst ab 16 Jahre, mit nat. Regel: ab 13 Jahre**
- **Opt-in erforderlich, keine Opt-out-Lösung möglich**
- **Gilt neben § 7 Abs. 3 UWG (E-Mail-Werbung)?**

Grundprinzip normale pbD

Einwilligung (lit. a) - Forts.

- Schwierig für öffentliche Hand - Vermutung fehlender Freiwilligkeit (EG 43)

EG 43

Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern. ……

Grundprinzip normale pbD

Rechtliche Verpflichtung (lit. c)

Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

…

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

Grundprinzip normale pbD

Öffentliches Interesse (lit. e)

Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

...

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

Grundprinzip normale pbD

Öffentliches Interesse (lit. e)

- **Verpflichtung und öffentliche Aufgabe müssen sich aus Rechtsvorschriften ergeben (Art. 6 Abs. 3 Satz 1 DS-GVO)**
  - Bundes- oder Landesrecht
- **Rechtsgrundlage muss weiteren Voraussetzungen genügen, vor allem**
  - muss Zweck der Datenverarbeitung angeben (Art. 6 Abs. 3 Satz 2 DS-GVO)
- **Widerspruchsrecht. Hinweispflicht (Art. 21 Abs. 4)!**

Grundprinzip normale pbD

Widerspruchsrecht

Niedrige Anforderungen an ein öffentliches bzw. berechtigtes Interesse werden durch Widerspruchsrecht kompensiert

„Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e [öffentliches Interesse] oder f [berechtigtes Interesse] erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling.

Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen." (Art. 21 Abs. 1)

Grundprinzip normale pbD

Widerruf / Widerspruch

Ermächtigungsgrundlage (Art. 6)	Beseitigungsmöglichkeit	
Vertragsdurchführung (Abs. 1 lit b)	Nicht möglich	
Einwilligung (Abs. 1 lit a)	Widerruf	Art. 7 Abs. 3 DSGVO
Öff. Interesse / berechtigtes Interesse (Abs. 1 lit e + lit f)	Grds. nicht möglich	
	Widerspruch Art. 21 DSGVO	Art. 21 Abs. 1 DSGVO Besondere Situation
		Art. 21 Abs. 2 DSGVO Direktwerbung

Grundprinzip normale pbD

Kompatibel mit ursprünglichem Zweck (Art. 6 Abs.4)

Verarbeitung ohne (neue) Ermächtigungsgrundlage zulässig, wenn

- mit ursprünglichem Zweck der Datenerhebung vereinbar (neu! Aufweichung!) - Kriterien für Vereinbarkeit (Art. 6 Abs. 4, vgl. auch EG 50)
  - Verbindung zwischen den Zwecken
  - Zusammenhang, in dem die pbD erhoben wurden, insbesondere Verhältnis Verantwortlicher und Betroffener
  - Art der pbD
  - Mögliche Folgen der beabsichtigten Weiterverarbeitung für betroffene Person
- wenn durch Einwilligung oder Rechtsvorschrift erlaubt => § 23 Abs. 1 Nr. 6 BDSG n.F.
- Pflicht zur Information des Betroffenen (Art. 14)

Grundprinzip besondere pbD

Verbot mit Ausnahmen

	Art. 9 Abs. 2 lit. a DSGVO	Einwilligung („ausdrücklich")	+ BDSG
Ge-setz	Art. 9 Abs. 2 lit. b DSGVO	Arbeitsrecht	+ BDSG
	Art. 9 Abs. 2 lit. c DSGVO	Schutz lebenswichtiger Interessen	
	Art. 9 Abs. 2 lit. d DSGVO	Organisation ohne Gewinnerzielungsabsicht	
	Art. 9 Abs. 2 lit. e DSGVO	pbD von Betr. offensichtlich öffentlich gemacht	
	Art. 9 Abs. 2 lit. f DSGVO	Geltendmachung oder Verteidigung gegen Rechtsansprüche(n)	
	Art. 9 Abs. 2 lit. g DSGVO	Öffentliches Interesse	+ BDSG
	Art. 9 Abs. 2 lit. h DSGVO	Gesundheitsvorsorge	+ BDSG
	Art. 9 Abs. 2 lit. i DSGVO	Öffentliches Interesse i. B. d. öffentlichen Gesundheit	+ BDSG
	Art. 9 Abs. 2 lit. j DSGVO	Forschungszwecke (Auflagen nach Abs. 3)	+ BDSG

Grundprinzip besondere pbD

Besondere personenbezogene Daten

„... rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen...Gewerkschaftszugehörigkeit.... Genetische... Daten [Def. Art. 4 Nr. 13; Erwägungsgrund 34], biometrische... Daten [Def. Art. 4 Nr. 14] zur eindeutigen Identifizierung einer natürlichen Person , Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person...“ (Art. 9 Abs. 1, Unterschiede zu § 3 Abs 9 BDSG a.F. hervorgehoben)

Grundsätze

- gelten neben Art. 6 bzw. Art. 9 / 10
- massiv bußgeldbewehrt

Überblick

- **Grundsätze für die Verarbeitung personenbezogener Daten, Art. 5 Abs. 1**
  - a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  - b) Zweckbindung (keine eigenmächtige Erweiterung)
  - c) Datenminimierung (auf Notwendiges – Zweck! – beschränkt)
  - d) (sachliche) Richtigkeit, Aktualität
  - e) (zeitliche) Speicherbegrenzung
  - f) Integrität und Vertraulichkeit
- Rechenschaftspflicht (Dokumentation!), § 5 Abs. 2

Durchführung des Beschäftigungsverhältnisses

Veröffentlichung von Mitarbeiterdaten allgemein

Basiskommunikationsdaten	Personenzusatzdaten
• Name	Konfession
• Funktions-/Tätigkeitsbereich	Geburtsdaten
• Dienstanschrift	Berufsabschluss
• E-Mail-Adresse	
Telefon-, Faxnummer	

- -> Bereitstellung der Daten bei Funktionsträgern auch ohne Einwilligung möglich
- Bei Nicht-Funktionsträgern **nicht „erforderlich“**, ohne Einwilligung unzulässig!

- -> Ohne Einwilligung immer unzulässig!

Betroffenenrechte

Überblick

- Informationspflicht bei Direkterhebung pbD (Art. 13)
- Informationspflicht bei Erhebung pbD bei Dritten (Artikel 14)
- Auskunftsrecht der betroffenen Person (Artikel 15)
- Recht auf Berichtigung (Art. 16)
- Recht auf Löschung - "Recht auf Vergessenwerden“ (Artikel 17)
- Recht auf Einschränkung der Verarbeitung (Artikel 18)
- Recht auf Datenübertragbarkeit (Artikel 20)
- Widerspruchsrecht (Artikel 21)

Betroffenenrechte

- Deutlich gestiegener Aufwand
- Bußgeldbewehrt!

Informationspflichten (Art. 13-14)

Regelungspunkt	Art. 13 Erhebung von pbD beim Betroffenen	Art. 14 Erhebung von pbD nicht beim Betroffenen
Obligatorische Daten (Abs. 1)	• die Tatsache der Datenerhebung • Verantwortlicher: Identität + Kontaktdaten • ggf. Kontaktdaten DSB • die Zwecke der Datenverarbeitung • Rechtsgrundlage • ggf. das berechtigtes Interesse an der Datenverarbeitung (Art. 6 Abs. 1 f) • die Empfänger oder Kategorien von Empfängern im Falle der Datenübermittlung, • (im Falle der Drittstaatenübermittlung) die von ihm getroffenen „safeguards“	wie Art. 13 mit folgender Abweichung • nicht: ggf. das berechtigte Interesse an der Datenverarbeitung (Art. 6 Abs. 1 f) • zusätzlich: die Kategorien pbD, die verarbeitet werden
Notwendig…, um „faire und transparente Verarbeitung zu gewährleisten“ (Abs. 2) = immer? (GDD)	• Die Speicherfrist • die Auskunfts- Berichtigungs- Vervollständigungs-, Löschungs-, Verarbeitungsbeschränkungs-, Widerspruchs- und Datenportabilitätsrechte des Betroffenen • das Recht des Betroffenen, die Einwilligung zu widerrufen • das Recht, eine Beschwerde bei der Datenschutzaufsicht einzureichen • ggf. Pflicht, Daten bereitzustellen • (im Falle der automatisierten Einzelfallentscheidung) die Logik der Datenverarbeitung (gesamter Algorithmus, Erwägungsgrund 63; a.A. noch BGH, Urteil vom 28.1.2014 - Schufa)	wie Art. 13 mit folgender Abweichung • nicht: ggf. Pflicht, Daten bereitzustellen • zusätzlich: – ggf. das berechtigte Interesse an der Datenverarbeitung (Art. 6 Abs. 1 f) – aus welcher Quelle die pbD stammen, ggf., ob aus öffentlichen Quellen stammend

Betroffenenrechte

Informationspflichten (Art. 13-14) - Forts.

Regelungspunkt	Art. 13 Erhebung von pbD beim Betroffenen	Art. 14 Erhebung von pbD nicht beim Betroffenen
bei Weiterv.	Tatsache der beabsichtigten Weiterverarbeitung und alle hier genannten Informationen auch für die Weiterverarbeitung (Abs. 3 bzw. Abs. 4)	
Einschränkung	Betroffener verfügt bereits über Info (Abs. 4)	• Betroffener verfügt bereits über Info • VHM • gesetzliche Regelung etc. (Abs. 5)
Zeitpunkt	• bei Datenerhebung • jederzeit auf Ersuchen des Betroffenen, kostenlos (Art. 15)	• angemessene Frist, spätestens 1 Monat • spätestens bei erster Mitteilung an Betroffenen bzw. erster Offenlegung an Dritte • jederzeit auf Ersuchen des Betroffenen

+ BDSG

Betroffenenrechte

Auskunftspflicht (Art. 15)

Punkt	Regelung
Inhalt	• Zweck • Daten/-kategorien • Empfänger/-kategorien • Speicherdauer • Betroffenenrechte • Herkunft der Daten • Evtl. automatisierte Entscheidung • Übermittlung in Drittstaaten + BDSG
Frequenz	• In angemessenen Abständen (z.B. jährlich)
Form	• bei Antrag in elektronischer Form auf gängigem elektronischem Weg • ggf. Fernzugang zu einem sicheren System (direkter Zugriff) • keine Beeinträchtigung der Rechte und Freiheiten anderer Personen (auch Gewerbliche Schutzrechte, Urheberrechte, Betriebs- und Geschäftsgeheimnisse) • Ggf. Kopie aller personenbezogenen Daten

Betroffenenrechte

Recht auf Löschung / „Vergessenwerden“

Betroffene Person kann die unverzügliche Löschung verlangen

- Daten sind für Erhebungszwecke nicht mehr erforderlich
- Widerruf der Einwilligung und keine anderweitige Rechtsgrundlage
- Zulässiger Widerspruch gemäß Art. 21 Abs. 1 oder 2
- Einwilligung eines Kindes in Dienste der Informationsgesellschaft gem. Art. 8 Abs. 1

- ggf. Ausnahmen gemäß Art. 15 Abs. 3 oder aufgrund nationaler bzw. spezieller Vorschriften, z.B. bei rechtlicher Verpflichtung zur Verarbeitung, Verarbeitung im öffentlichen Interesse, Forschung (vgl. auch § 35 BDSG n.F.)

Betroffenenrechte

Recht auf Einschränkung

Einschränkung

- Richtigkeit der Daten wird bestritten
- Verarbeitung ist unrechtmäßig, Betroffener lehnt aber Löschung ab
- Daten erforderlich im Zusammenhang mit Rechtsansprüchen (z.B. Archivierung)
- Prüfung der Zulässigkeit eines Widerspruchs (Interessenabwägung)

Wurde die Verarbeitung gemäß Absatz 1 eingeschränkt, so dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden." (Art. 18 Abs. 2)

Verzeichnis v. Verarbeitungstätigkeiten

- Zentrales Management-Tool
- Bußgeldbewehrt!

- von Verantwortlichem und ggf. AV (Art. 30 Abs. 1, 2) zu erstellen und zu führen
- Anwendungsbereich nur scheinbar aufgelockert (Art. 30 Abs. 5)

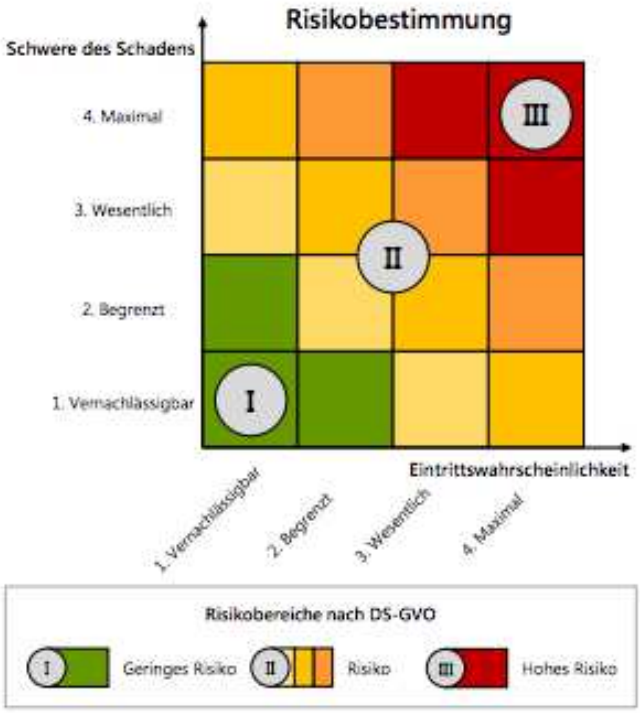
  „… es sei denn, … die Verarbeitung erfolgt nicht nur gelegentlich…." – Ausnahmetatbestände sind alternativ!
- Sämtliche Verarbeitungstätigkeiten erfassen (Art. 30 Abs. 1)
- Hilfreich zur Erfassung Ausrichtung an:
  - Geschäftsprozessen (empfohlen von Bitkom)
  - Verarbeitungszwecken
  - Systemen (Hard- und Software)
- Empfohlener Inhalt:
  - Pflichtangaben
  - Erweiterte Angaben (Hilfe für Erfüllung Informations- und Dokumentationspflicht)

Verzeichnis v. Verarbeitungstätigkeiten

Typische Verarbeitungstätigkeiten in Unternehmen

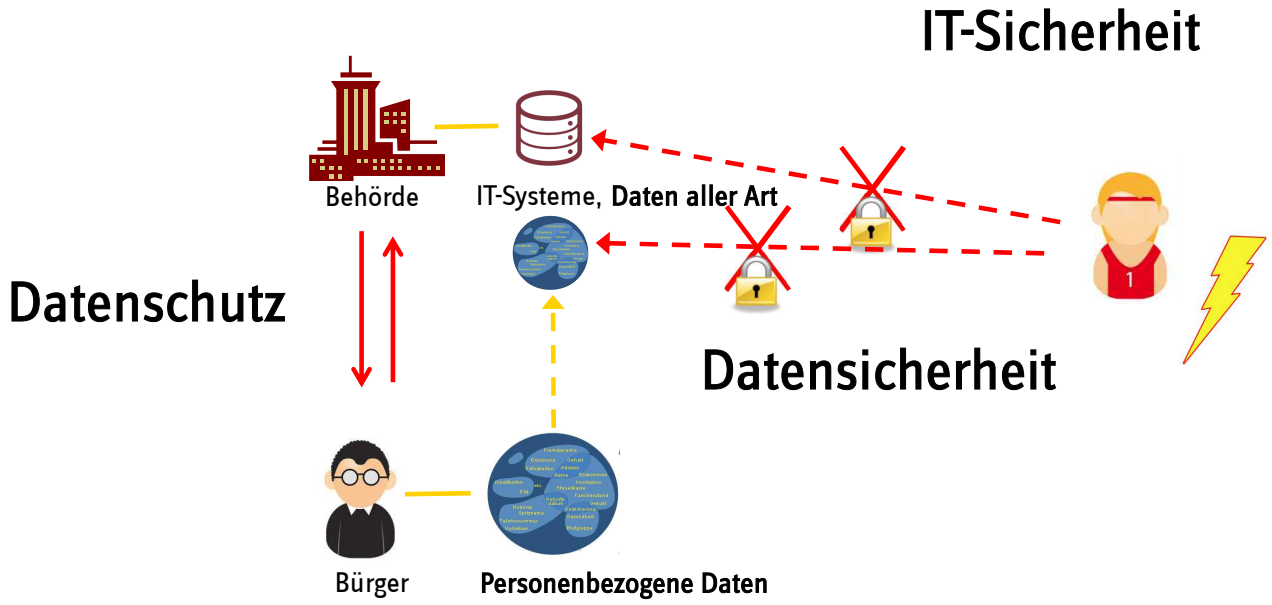
- Bewerbermanagement
- Personalmanagement
- Lohnabrechnung
- Reisemanagement
- Fuhrparkmanagement
- Marketing und Vertrieb
- Leistungserbringung
- Rechnungslegung
- Zahlungsabwicklung
- Mahnwesen
- Kundenbetreuung
- CRM-System
- Beschaffung (inkl. IT)
- Akten- und Datenvernichtung
- IT-Leistungen, Softwareadministration, Support
- Tk-Leistungen
- Finanzbuchhaltung
- Unternehmens-, Objekt- und Informationssicherheit

Datenschutzfolgenabschätzung



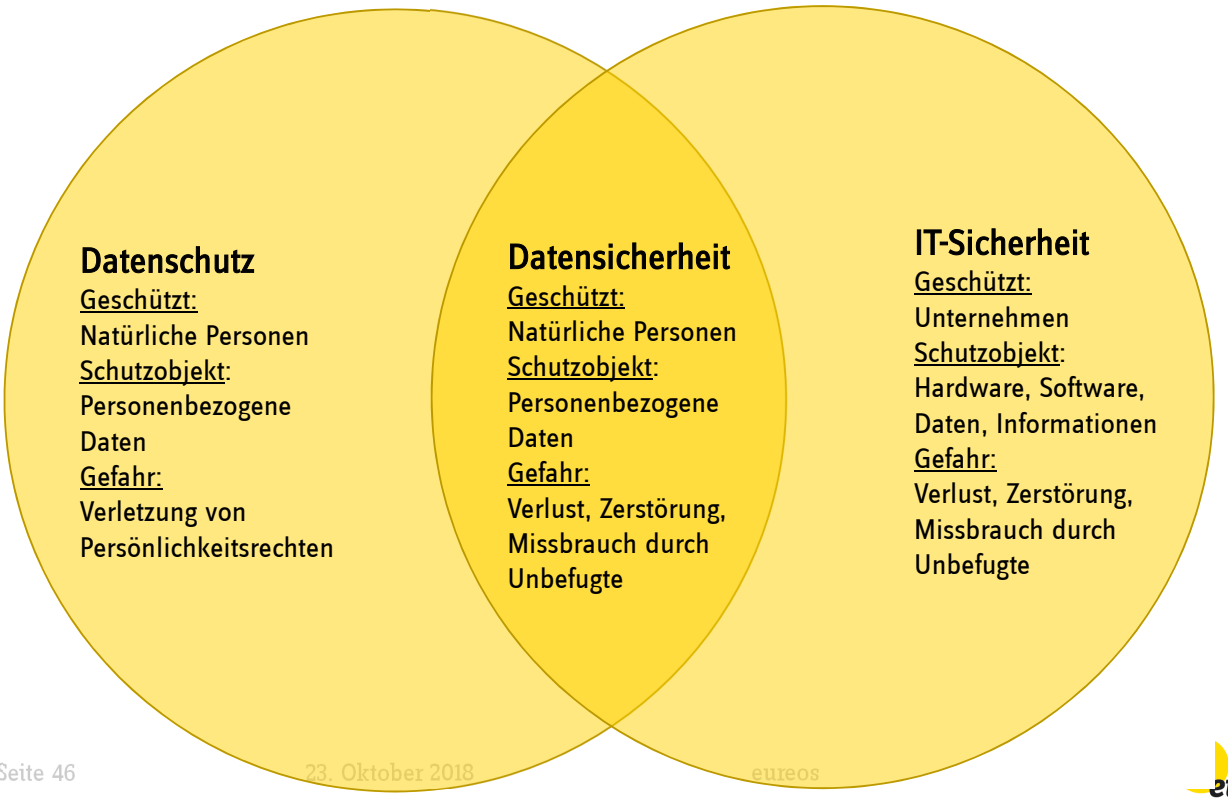
Quelle: BLaDSA

Datensicherheit



Quelle: http://www.grafiker.de/kreativ-news/02092009/people-icon-set-klappe-die-dritte; https://www3.sachsen.schule/thema-datenschutz/start/

Datensicherheit



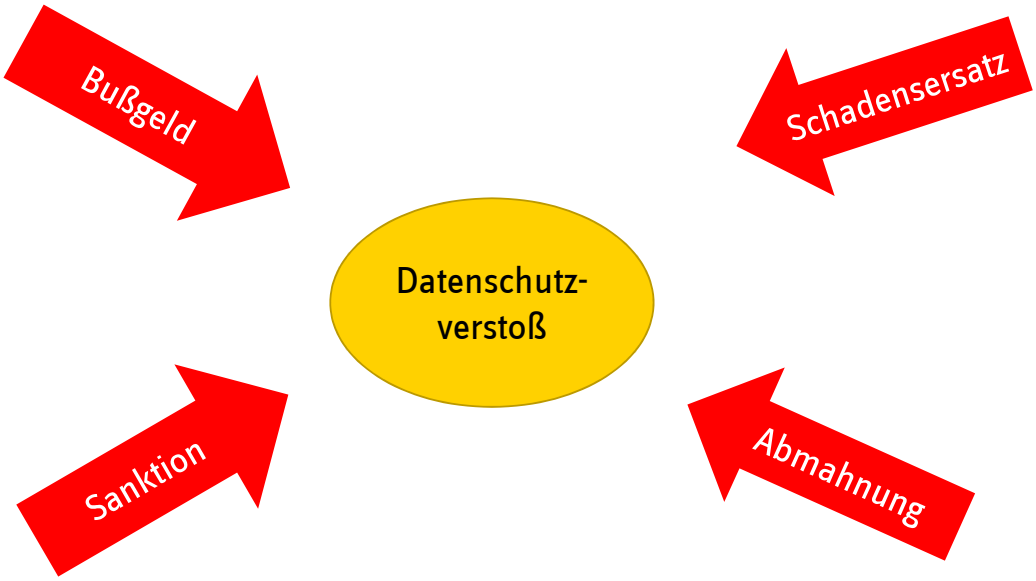
Datensicherheit

Schutzziele und TOM's

Schutzziel	Definition	Maßnahmen
Vertraulich-keit	nur Befugte können pbD / D zur Kenntnis nehmen	Passwortschutz, Alarmanlage/Videoüberwachung/Pförtner, Zutrittsschutz, VPN, Virenschutz/Firewall, Sperrung von Schnittstellen (z.B. USB), Pseudonymisierung, Verschlüsselung, Vertraulichkeitsregelungen
Integrität	pbD / D bleiben während der Verarbeitung unversehrt, vollständig und aktuell	Rollen/Rechtekonzept, Protokollierungen
Verfügbarkeit	pbD / D stehen zeitgerecht zur Verfügung und können ordnungsgemäß verarbeitet werden	Auslagerung von Sicherungskopien, Notstrom-Aggregate, unterbrechungsfreie Stromversorgung, Sicherungen gegen Elementarschäden,
Belastbarkeit	Begriff nicht definiert	Notfallplan, Penetrationstest, Anpassungsfähigkeit

- Vgl. Art. 32 Abs. 1 lit. b, EG 78

Risiken Datenschutz Non-Compliance



II. Praktische Fälle Asylhilfe

Fotos

Fotos

Recht am eigenen Bild / Datenschutz der Abgebildeten

Artikel 9 Abs. 1 DS-GVO: *Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, [...]* ***ist untersagt.***

Datenschutzinformation

BAMF-Information Asylverfahren (1/2)

Am 25.05.2018 ist die Datenschutzgrundverordnung (DSGVO) in Kraft getreten. Neben den Informationspflichten des Bundesamtes ergeben sich nach Art. 15 bis 22 und Art. 34 DSGVO zusätzliche Auskunftspflichten des Bundesamtes.

Wenn Sie Asyl beantragen, sind Sie nach dem Gesetz verpflichtet, dem Bundesamt bestimmte persönliche Daten zu geben. Wenn Sie das nicht tun, kann es sein, dass Ihr Asylverfahren eingestellt werden muss. Es kann auch sein, dass Ihr Asylantrag abgelehnt wird oder dass Ihre Leistungen als Asylbewerber gekürzt werden.

Ihre Daten werden vom Bundesamt für Ihr Asylverfahren weiter verarbeitet und an Gerichte und andere Behörden weitergegeben. Das Bundesamt ist hierzu nach dem Gesetz berechtigt und verpflichtet. Auch an andere Staaten und nichtstaatliche Organisationen können die Daten übermittelt werden. Das alles geschieht natürlich nur, wenn das für Ihr Asylverfahren notwendig und rechtlich zulässig ist. Die im Asylverfahren gemachten Angaben werden nicht den Behörden Ihres Herkunftslandes mitgeteilt

Spätestens zehn Jahre nachdem Ihr Asylverfahren abgeschlossen wurde oder nachdem Sie Deutschland verlassen haben, werden Ihre Daten gelöscht.

Sie können jederzeit erfahren, welche Daten wir von Ihnen haben und verarbeiten. Außerdem können Sie eine Berichtigung Ihrer Daten beantragen. In diesen Fällen schreiben Sie eine E-Mail an uns.

Datenschutzinformation

BAMF-Information Asylverfahren (2/2)

Das Bundesamt darf Daten erheben, wenn es diese Daten für seine Arbeit benötigt. Diese Daten werden verarbeitet im:

Bundesamt für Migration und Flüchtlinge
Frankenstraße 210
90461 Nürnberg

Für den Datenschutz im Bundesamt gibt es einen Datenschutzbeauftragten. Seine Anschrift ist:

Datenschutzbeauftragter
Bundesamt für Migration un d Flüchtlinge
Frankenstraße 210
90461 Nürnberg

Beschwerden können Sie an folgende Adresse richten:

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Husarenstr. 30
53117 Bonn

Datum 25.05.2018

http://www.bamf.de/DE/Fluechtlingsschutz/InformationenFuerGefluechtete/informationen-nach-dsgvo-asylverfahren.html

Verbände und andere Helfer

Herausgabe von pbD von Asylbewerbern von Behörden an Wohlfahrtsverbände und ehrenamtliche Helfer?

- **„Ohne wirksame Einwilligung der Betroffenen halte ich dies für nicht zulässig, da weder das Bayerische Datenschutzgesetz noch eine andere Rechtsvorschrift die Übermittlung erlaubt oder anordnet. Insbesondere erfordert es die Unterstützung der neu ankommenden Asylbewerber bei der Erfüllung melderechtlicher Pflichten nicht, einen Überblick über alle etwa im Landkreis untergebrachten Asylbewerber zu haben. Insoweit wäre die Übermittlung der vom Landratsamt geführten Listen unverhältnismäßig. Grundsätzlich erscheint es angesichts des Umfangs und der Sensibilität der in solchen Listen aufgeführten personenbezogenen Daten angezeigt, den Kreis der Listeninhaber so klein wie möglich zu halten, auch um die Gefahr eines etwaigen Missbrauchs nicht zu erhöhen.**

- **Selbstverständlich dürfen die Wohlfahrtsverbände und ehrenamtlichen Helferkreise ihre Hilfsangebote in allgemeiner Form an die Asylbewerber herantragen. Diese können dann selbst darüber entscheiden, ob und inwieweit sie eine Kontaktaufnahme bzw. eine Unterstützung wünschen. Insoweit halte ich es für vertretbar, dass die Anschriften der dezentralen Unterkünfte an die Wohlfahrtsverbände weitergegeben werden, ggf. verbunden mit der Angabe, wie viele Asylbewerber aus welchen Nationen dort jeweils untergebracht sind.“ (BayLfD: FAQ - Beratung und Betreuung von Asylbewerbern)**

Verbände und andere Helfer

Dürfen Helferkreise eine eigene Datenbank aufbauen?

Verbände und andere Helfer

Dürfen Krankenhäuser Patientendaten von Asylbewerbern an Sozialbetreuer herausgeben?

- „Die soziale Betreuung von Asylbewerbern durch Angehörige von Wohlfahrtsverbänden oder von ehrenamtlichen Helferkreisen ist nicht mit der rechtlichen Betreuung im Sinne der §§ 1896 ff. Bürgerliches Gesetzbuch vergleichbar. Insbesondere ergibt sich aus einem freiwilligen Betreuungsverhältnis - anders als bei der gerichtlich angeordneten Betreuung - regelmäßig keine Vertretungsmacht nach außen.
- Insofern besteht für die Sozialbetreuer auch keine generelle Vollmacht zur Entgegennahme von Auskünften über den Gesundheitszustand der von ihnen betreuten Asylbewerber. Stehen die Auskünfte im Zusammenhang mit einem Krankenhausaufenthalt, bedarf die Übermittlung von Patientendaten an Sozialbetreuer grundsätzlich der ausdrücklichen Einwilligung der Asylbewerber. Nach den Umständen des Einzelfalls kann auch eine konkludente Einwilligung in Betracht kommen, etwa wenn Asylbewerber in Begleitung von Sozialbetreuern zur Behandlung ins Krankenhaus kommen.“ (BayLfD: FAQ - Beratung und Betreuung von Asylbewerbern)

Datensicherheit

Risiken im Asyl-Aktensystem

- System Maris (Migrations-Asyl-Reintegrationssystem): erfasst den Namen, die Staatsangehörigkeit, das Aktenzeichen, Scans wichtiger Schriftstücke, das Protokoll der Anhörung oder die Adresse des Schutzsuchenden. Mehr als 2,5 Millionen Akten sind heute im System gespeichert.
- Risiken: weitreichende Zugriffsbefugnisse von Mitarbeitern, keine Protokollierung der Zugriffe, fehlende Möglichkeit zur Sperrung bestimmter Daten
  - Rund die Hälfte aller BAMF-Mitarbeiter können Asylakten weitreichend „umprotokollieren“ => Mißbrauchsmöglichkeit, eigentlich geplante Anhörung kann z.B. verhindert werden
  - Zugriffe auf Maris können nicht nachvollzogen werden, weil diese lediglich auf dem jeweiligen Rechner und nicht zentral auf einem Server protokolliert wurden => Spione könnten unbemerkt Informationen über Regimegegner sammeln

Datenträgerauswertung

§ 15a AsylG neue Fassung

- Auswertung von Datenträgern (Handys etc.) von Asylbewerbern möglich
- Erhebliche Kritik von Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (umfassende Auswertungsmöglichkeiten) nicht berücksichtigt.

(1) Die Auswertung von Datenträgern ist nur zulässig, soweit dies für die Feststellung der Identität und Staatsangehörigkeit des Ausländers nach § 15 Abs. 2 Nr. 6 erforderlich ist und der Zweck der Maßnahme nicht durch mildere Mittel erreicht werden kann. § 48 Abs. 3a Satz 2 bis 8 und § 48a des Aufenthaltsgesetzes gelten entsprechend.
(2) Für die in Absatz 1 genannten Maßnahmen ist das Bundesamt zuständig.

Fälle aus der Praxis der Teilnehmer

- Fälle
- Diskussion

Vielen Dank

Dierk Schlosshan
Rechtsanwalt

eureos gmbh
steuerberatungsgesellschaft
rechtsanwaltsgesellschaft

Telefon: + 49 (351) 4976 1519
d.schlosshan@eureos.de
→ **www.eureos.de**