Neues EU-Datenschutzrecht im Bereich des Vollstreckungswesens

Birgit Pauls, behördliche Datenschutzbeauftragte
10. Juli 2019, Bundesarbeitstagung 2019 in Würzburg

Inhalt

- Typische Aussagen zum Datenschutz
- Grundlagen Datenschutz
- Rechte der Betroffenen
- technische und organisatorische Maßnahmen
- Besonderheiten im Vollstreckungswesen

Typische Aussagen zum Datenschutz

Datenschutz ist Schuldnerschutz!

O-Ton eines Vollstreckungsbeamten am ersten Arbeitstag seiner Datenschutzbeauftragten

Man kommt nicht an die Daten der Schuldner ran…

Grundrecht Datenschutz

Artikel 8 Abs. 1 EU Grundrechtecharta:

Jede Person hat das Recht auf den Schutz der sie betreffenden personenbezogenen Daten.

Spezialfall Vollstreckung

- Datenübermittlungen zur Vollstreckung öffentlich-rechtlicher Forderungen sind häufig möglich
- Es muss nur die richtige Rechtsgrundlage angewendet werden
- Beispiel Sozialdatenschutz:
  § 74a SGB X: Übermittlung zur Durchsetzung öffentlich-rechtlicher Ansprüche und im Vollstreckungsverfahren

Wir müssen jetzt den Datenschutz einhalten

Datenschutz ist nichts Neues

- Eid des Hippokrates
- Beichtgeheimnis (1215)
- Postgeheimnis / Briefgeheimnis (ca. 1700)
- Fernmeldegeheimnis
- Steuergeheimnis
- Landesdatenschutzgesetz Hessen (1970)
  → weltweit erstes Datenschutzgesetz
- Bundesdatenschutzgesetz (1977)
- EU-Datenschutzrichtlinie (1995)

Wir dürfen nicht mehr wegen Datenschutz…
Wir brauchen für alles Einwilligungen…

Zulässigkeit der Verarbeitung

- Verarbeitungen, die vor der DSGVO zulässig waren, sind es in der Regel auch heute
- Rechtsgrundlagen für Zulässigkeit ähnlich wie vorher
- Ziele der DSGVO
  - → Modernisierung des Datenschutzes, Anpassung an die technischen Möglichkeiten, Ende des „Lochkartenzeitalters“
  - → Einheitliches Datenschutzrecht in Europa
  - → Erleichterungen für Unternehmen bzgl. Datentransfer innerhalb der EU
  - → Stärkung Verbraucherschutz

Es wird jetzt teuer und kompliziert …

Schon seit 197x im Gesetz:

- Rechtsgrundlage für Verarbeitung notwendig
- Mindestanforderungen an technische und organisatorische Maßnahmen
- Vertragsgestaltung bei Auftrags-(daten-)Verarbeitung
- Rechte der Betroffenen
- Dokumentationspflichten (ergaben sich auch aus Spezialgesetzen)
- Pflicht zur Bestellung von Datenschutzbeauftragten (Abweichungen in Landesdatenschutzgesetzen)

Es gibt wenig Neues…

- Datenschutz Folgenabschätzungen durch den Fachbereich statt Vorabkontrolle durch den Datenschutzbeauftragten
- Transparenzanforderungen erhöht
- Datenübertragbarkeit → bei öffentlichen Stellen meist nicht anwendbar
- Privacy by Design and Default
- Rechenschaftspflicht
- Ersatz für immaterielle Schäden bei Datenschutzverletzungen

Grundlagen Datenschutz

Gesetzliche Grundlagen

- EU Datenschutz Grundverordnung (DSGVO)
- Ergänzend zur Ausgestaltung von Öffnungsklauseln:
  → Bundesdatenschutzgesetz (§§ 1- 44)
  → Landesdatenschutzgesetze
- Spezialgesetze
  → Abgabenordnung
  → Sozialgesetzbücher
  → Bundesmeldegesetz
  → Kommunalabgabengesetze der Länder
  → Landesverwaltungsgesetze
  → Regelungen zur Vollstreckung

JI-Richtline

- Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI
- Umgesetzt im BDSG ab § 45 sowie Ländergesetzen
- Betrifft hauptsächlich Polizei und Justiz, aber auch Verfolgung von Ordnungswidrigkeiten erfasst

Anforderungen an Verarbeitung

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Rechenschaftspflicht

- Art. 5 Abs. 2 DSGVO: Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können
- Revisionssichere Dokumentation
- Klassisches Qualitätsmanagement
- Entsprechende Regelungen vor DSGVO auch schon in Spezialgesetzen vorhanden,
  z.B. § 36 Abs. 2 Nr. 4 GemHVO Doppik SH
  Sicherheitsstandards und Dienstanweisung

Verbot mit Erlaubnisvorbehalt

- Einwilligung des Betroffenen
- Vertrag oder vorvertragliche Verhandlungen
- Auf Grund einer gesetzlichen Regelung, der der Verantwortliche unterliegt
- Zum Schutz lebenswichtiger Interessen des Betroffenen oder einer anderen Person
- Zur Erfüllung im öffentlichen Interessen liegenden Ausgaben
- Bei berechtigtem Interesse des Verantwortlichen, sofern Schutz der Interessen der betroffenen Person nicht überwiegen (nicht für Behörden bei Aufgabenerfüllung)

Rechte der Betroffenen

Transparenz

- geeignete Maßnahmen, um der betroffenen Person alle Informationen zu übermitteln
- In präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln
- insbesondere für Informationen, die sich speziell an Kinder richten.

Fristen

- Angeforderte Informationen müssen unverzüglich zur Verfügung gestellt werden
- Spätestens innerhalb eines Monats nach Eingang des Antrages
- Frist kann um zwei Monate verlängert werden, dann ist die Person unter Angabe der Gründe zu informieren

Information bei Erhebung

- Betroffene müssen bei Datenerhebung (Direkt oder bei Dritten) informiert werden
- Mindestangaben siehe Art. 13, 14 DSGVO
- In einigen Fällen Ausnahmen möglich
- „Datenschutzhinweise“ bezogen auf das Verfahren
- Kurzinformationen auf Bescheiden mit dem Hinweis, wo die vollständigen Informationen zu finden sind
- Hilfestellungen in den Kurzpapieren 6, 10 und 11 der Datenschutzkonferenz (DSK)
- „Datenschutzsteckbrief“ ULD Schleswig-Holstein

Auskunft

- Allgemeiner kostenloser Anspruch auf Auskunft des Betroffenen
- Nicht zu verwechseln mit dem Recht auf Akteneinsicht (gilt nur für einen begrenzten Zeitraum)
- In Ausnahmefällen keine Auskunft erforderlich
- Betroffener soll Daten, die beauskunftet werden sollen, so genau wie möglich benennen
- Betroffener muss sich identifizieren
- Achtung: keine Daten anderer Betroffener benennen

Löschung

- Erforderlich, wenn Zwecke für die Verarbeitung entfallen sind (Datenminimierung)
- Sperren (Einschränkung der Verarbeitung) nur noch in Ausnahmefällen zulässig
- Problematik: Echtes Löschen technisch schwer möglich
- Vor dem Löschen gesetzliche Aufbewahrungsfristen und Archivanbietungspflichten beachten
- „Recht auf Vergessenwerden“: bei Übermittlungen müssen Empfänger informiert werden

Berichtigung

- Unverzügliche Berichtigung falscher Daten
- Ergänzung unvollständiger Daten unter Berücksichtigung des Zweckes der Verarbeitung

Widerspruchsrecht

- Bei Gründen, die sich aus einer besonderen Situation ergeben ist Widerspruch gegen Verarbeitung nach Art. 6 Abs. 1 e, f DSGVO möglich, wenn Rechtsgrundlage für Verarbeitung ist:
  - → Erfüllung einer öffentlichen Aufgabe
  - → Wahrung berechtigter Interessen des Verantwortlichen
- Nicht zu verwechseln mit dem Recht, Einwilligungen jederzeit mit Wirkung für die Zukunft zu widerrufen

Datenübertragbarkeit

- Nur bei Daten, die auf Grund von Einwilligung oder Vertrag verarbeitet werden
- Betroffener kann auf Anforderung Daten in einem gängigen maschinenlesbaren Format erhalten
- In der Regel bei Behörden mit Datenverarbeitung zum Zwecke der Aufgabenerfüllung nicht anwendbar

Datenpannen

- Meldung von Verletzungen des Schutzes personenbezogener Daten an die zuständige Datenschutzaufsichtsbehörde immer innerhalb 72 Stunden, wenn Risiken für Rechte und Freiheiten der Betroffenen bestehen, Verzögerung muss begründet werden (Artikel 33 DSGVO)
- Bei hohem Risiko für die Betroffenen müssen die Betroffenen informiert werden
  → Bei Daten zu Vollstreckung in der Regel hohes Risiko

Technische und organisatorische Maßnahmen

Anforderungen DSGVO

- Technische und organisatorische Maßnahmen sind zu treffen unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt (Art. 24 DSGVO)

Etwas Genauer …

Artikel 32 DSGVO

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die **Vertraulichkeit, Integrität**, **Verfügbarkeit** und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen **Zwischenfall rasch wiederherzustellen**;

Ständige Verbesserung

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Privacy by Design & Default

- Datenschutzfreundliche Hard- und Softwarekonzepte, z.B. Beschränkung der Eingaben auf das Erforderliche, Einschränkung von Zugriffsberechtigungen technisch möglich
- Grundeinstellung: Keine Zugriffe erlaubt, Berechtigungen müssen entsprechend vergeben werden

Und woher nehmen wir jetzt konkrete Maßnahmen?

Ordnungsgemäße Buchhaltung

- Zugriffe abhängig von Aufgabe und Funktion, Funktionstrennung
  → Berechtigungskonzept
- Nachvollziehbarkeit von Buchungen
  → Protokollierung
- Manipulationssicherheit
  → Sicherstellung der Integrität, Protokollierung
- Spezialgesetze liefern Anforderungen analog zum Datenschutz, sind aber häufig viel konkreter (z.B. GemHVO Doppik)

BSI IT-Grundschutz

- Regelwerk zur Herstellung der IT-Sicherheit
  www.bsi.bund.de
- Zur Erfüllung der Anforderungen aus ISO 27001 (IT-Sicherheit)
- Muss für Bundesbehörden
- Empfehlung: Auch in anderen Verwaltungen nutzen.
  § 5 OZG fordert indirekt BSI IT-Grundschutz
- Bzgl. Datenschutz fordert BSI IT-Grundschutz die Anwendung des Standard Datenschutzmodels
  vgl. Baustein CON.2 Datenschutz

Standard Datenschutzmodell

- Enthält generische Maßnahmen zum Erreichen der sechs (Datenschutz-) Gewährleistungsziele

  Integrität, Vertraulichkeit, Verfügbarkeit

  Transparenz, Intervenierbarkeit, Nicht-Verkettbarkeit
- Zum Teil schon konkrete Maßnahmenkataloge veröffentlicht
  https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Besonderheiten im Vollstreckungswesen

Berücksichtigen

- Zulässigkeit der Datenerhebung und Übermittlung durch andere Stellen
- Grundsatz der Zweckbindung
- Grundsatz der Erforderlichkeit
  - → Datenminimierung
  - → Grundrechtseingriff so schonend wie möglich
  - → Direkterhebung beim Schuldner, wenn möglich
  - → keine unangemessene Belastung des Schuldners

Datenschutz blockiert?

- Datenschutz schützt den Schuldner nicht davor, seinen Zahlungsverpflichtungen nachzukommen
- Zahlreiche Rechtsgrundlagen zur Übermittlung in Spezialgesetzen
- Empfänger muss rechtliches Interessen an Übermittlung plausibel glaubhaft machen
- Aufhebung der Zweckbindung unter bestimmten Voraussetzungen in DSGVO, BDSG und LDSGs vorgesehen
- Nutzung öffentlich zugänglicher Quellen möglich

Bereichsspezifisch

- Vorrang der Bereichsspezifischen Regelungen vor BDSG, LDSGs
- § 882f ZPO Einsicht in das Schuldnerverzeichnis
- § 5a VwVG Ermittlung des Aufenthaltsorts des Vollstreckungsschuldners
- § 5b VwVG Auskunftsrechte der Vollstreckungsbehörde
- Landesverwaltungsgesetze
- § 74a SGB X
- … und weitere bereichsspezifische Regelungen

Fragen – bitte!