Anforderungen an die Dokumentation im Lichte der datenschutzrechtlichen Änderungen

Christian Prietz
ULD

Moderation:
Harald Zwingelberg ULD

Grundsätze für die Verarbeitung personenbezogener Daten (pbD)

Art. 5 Abs. 2 DSGVO

Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung **nachweisen** können („Rechenschaftspflicht“).

Grundsätze für die Verarbeitung pbD

- Aus Art. 5 Abs. 2 DSGVO folgt (zumindest) eine (in)direkte Pflicht zur Dokumentation

- Es sollte grundsätzlich dokumentiert werden bei:
  - Entsprechenden Anforderungen im Gesetz
  - Bei Abwägungsentscheidungen
  - Bei Begründungspflichten
  - Anderen Nachweispflichten

Auftragsdatenverarbeitung
<->
Auftragsverarbeiter

Auftragsdatenverarbeitung <-> Auftragsverarbeiter

Alte Rechtslage § 11 BDSG	Neue Rechtslage Art. 28 DSGVO
Vertrag notwendig	Vertrag notwendig (oder anderes Rechtsinstrument)
• Gegenstand und Dauer des Auftrags • Umfang, Art und Zweck der Verarbeitung • TOM nach § 9 BDSG • Art der personenbezogenen Daten • Berichtigung, Sperrung, Löschung von Daten • Begründung von Unterauftragsverhältnissen • Kontrollrechte des Auftraggebers • Mitzuteilende Verstöße des Auftragnehmers • Umfang der Weisungsbefugnisse des Auftragnehmers • Rückgabe überlassener Datenträger	• Gegenstand und Dauer der Verarbeitung • Art und Zweck der Verarbeitung • Art der personenbezogenen Daten • Kategorie betroffener Personen • Pflichten und Rechte des Verantwortlichen • Verarbeitung nur auf und entsprechend von dokumentierten Weisungen • Vertraulichkeits-, Verschwiegenheitserklärung der Mitarbeiter • Erforderliche Maßnahmen gem. Art. 32 DSGVO • Unterstützung des Auftraggebers (durch TOM) bei Anfragen des Betroffenen zur Rechtsdurchsetzung

Auftragsdatenverarbeitung <-> Auftragsverarbeiter

Alte Rechtslage § 11 BDSG	Neue Rechtslage Art. 28 DSGVO
	• Unterstützung des Auftraggebers bei der Einhaltung der Pflichten gem. Artt. 32 bis 36 DSGVO • Löschung oder Rückgabe aller personenbezogenen Daten • Informationsrechte und Kontrollbefugnisse des Verantwortlichen

Verfahrensverzeichnis
<->
Verzeichnis der Verarbeitungstätigkeiten

Verfahrensverzeichnis <-> Verzeichnis der Verarbeitungstätigkeiten

Alte Rechtslage §§ 4d, 4e BDSG	Neue Rechtslage Art. 30 DSGVO

Vor Inbetriebnahme der zuständigen Aufsichtsbehörde zu melden (§ 4d Abs. 1 BDSG), wenn
• Keine DSB bestellt (Abs. 2)
• Mehr als neun Personen dauerhaft mit der Verarbeitung befasst und
  • Keine Einwilligung vorliegt oder
  • Nicht zur Durchführung eines rechtsgeschäftlichen Schuldverhältnisses
	Ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen (Abs. 4)

Auf Antrag jedermann zur Verfügung zu stellen (§ 4g Abs. 2 BDSG)	Kein „Jedermann-Verzeichnis“ mehr
Zu führen durch die verantwortliche Stelle	Zu führen durch: - jeden Verantwortlichen (Abs. 1) bzw. - jeden Auftragsverarbeiter (sofern vorhanden) (Abs. 2)

Verfahrensverzeichnis <-> Verzeichnis der Verarbeitungstätigkeiten

Alte Rechtslage §§ 4d, 4e BDSG	Neue Rechtslage Art. 30 DSGVO
Name des Verantwortlichen • Unternehmensleitung (Inhaber, Vorstände Geschäftsführer etc.) • Anschrift	Namen und die Kontaktdaten des Verantwortlichen [...] sowie eines etwaigen Datenschutzbeauftragten • Anschrift • Ggf. Angaben zu einem gemeinsam mit ihm Verantwortlichen • Zum Vertreter des Verantwortlichen
Zwecke der Erhebung, Verarbeitung und Nutzung	Die Zwecke der Verarbeitung

Verfahrensverzeichnis <-> Verzeichnis der Verarbeitungstätigkeiten

Alte Rechtslage §§ 4d, 4e BDSG	Neue Rechtslage Art. 30 DSGVO
Beschreibung der betroffenen Personengruppen und der Daten bzw. Datenkategorien	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
Empfänger oder Kategorien von Empfängern, denen Daten mitgeteilt werden	Die Kategorien von Empfängern (in der Vergangenheit oder der Zukunft)
Geplante Datenübermittlung in Drittstaaten	Gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

Verfahrensverzeichnis <-> Verzeichnis der Verarbeitungstätigkeiten

Alte Rechtslage §§ 4d, 4e BDSG	Neue Rechtslage Art. 30 DSGVO
Regelfristen für die Löschung der Daten	Wenn möglich: • Löschfristen oder • Fristen für die regelmäßige Überprüfung (s. EG 39)
Allgemeine Beschreibung der Maßnahmen zu § 9 BDSG	Möglichst eine allgemeine Beschreibung der TOMs gemäß Art. 32 Abs. 1 DSGVO

Informationspflicht bei unrechtmäßiger Kenntniserlangung

<->

Meldung von Verletzungen des Schutzes pbD

Informationspflicht bei unrechtmäßiger Kenntniserlangung<-> Meldung von Verletzungen des Schutzes pbD

Alte Rechtslage § 42a BDSG	Neue Rechtslage Artt. 33, 34 DSGVO
Informationspflicht für: • Besondere Arten pbD • pbD i. Z. m. einem Berufsgeheimnis • pbD i. z. m. strafbaren Handlungen oder Ordnungswidrigkeiten • pbD zu Bank- oder Kreditkartenkonten	Keine Einschränkung mehr auf besonders sensible Daten => Gilt für jede Form der pbD
Bei unrechtmäßiger Übermittlung oder unrechtmäßiger Kenntniserlangung durch Dritte	Verletzung des Schutzes pbD (Verletzung der Sicherheit, unbeabsichtigt/unrechtmäßig, die zu Vernichtung / Verlust / Veränderung / unbefugter Offenlegung / unbefugtem Zugang pbD führen)
Schwerwiegende Beeinträchtigungen für die Rechte/schutzwürdigen Interessen des Betroffenen	<u>Notwendig:</u> • Risiko für die Rechte und Freiheiten natürlicher Personen (Art. 33 DSGVO) • Voraussichtlich hohes Risiko für Rechte und Freiheiten des Betroffenen (Art. 34 DSGVO)

Informationspflicht bei unrechtmäßiger Kenntniserlangung<-> Meldung von Verletzungen des Schutzes pbD

Alte Rechtslage § 42a BDSG	Neue Rechtslage Artt. 33, 34 DSGVO
Unverzügliche Meldung an zuständige Aufsichtsbehörde sowie an Betroffene	• Unverzüglich möglichst binnen 72 Std. nach Bekanntwerden an Aufsichtsbehörde (Art. 33 DSGVO) • „unverzügliche“ Mitteilung an den Betroffenen (Art. 34 DSGVO)
Information an Betroffenen über Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderungen möglicher Folgen	• Art der Verletzung • Mindestens die in Art. 33 Abs. 3, b, c und d DSGVO gemachten Angaben und Maßnahmen (Art. 34 Abs. 2 DSGVO)
Zusätzlich an Aufsichtsbehörde: Information über mögliche nachteilige Folgen und ergriffene Maßnahmen	• Art der Verletzung (Kategorien / ungefähre Anzahl der betroffenen Personen und Datensätze) (Art. 33 Abs. 3 a DSGVO) • Namen/Kontaktdaten des DSB bzw. einer sonstigen Anlaufstelle für weitere Informationen (Art. 33 Abs. 3 b DSGVO)

Informationspflicht bei unrechtmäßiger Kenntniserlangung<-> Meldung von Verletzungen des Schutzes pbD

Alte Rechtslage § 42a BDSG	Neue Rechtslage Artt. 33, 34 DSGVO
	• Beschreibung der wahrscheinlichen Folgen der Verletzung (Art. 33 Abs. 3 c DSGVO) • Beschreibung der ergriffenen / vorgeschlagenen Maßnahmen zur Behebung der Verletzung (Art. 33 Abs. 3 d DSGVO) • Maßnahmen zur Abmilderung möglicher nachteiliger Auswirkungen (Art. 33 Abs. 3 d)
	Es reicht ein bestimmter Grad der Wahrscheinlichkeit, positive Feststellung ist nicht zwingend notwendig => Ermittlungspflicht über das Ob und die Details
	Nach Art. 33 Abs. 5: Dokumentation über die Datenschutzverletzung, alle mit ihr, ihren Auswirkungen und ergriffenen Abhilfemaß-nahmen im Zusammenhang stehende Fakten

Informationspflicht bei unrechtmäßiger Kenntniserlangung<-> Meldung von Verletzungen des Schutzes pbD

Alte Rechtslage § 42a BDSG	Neue Rechtslage Artt. 33, 34 DSGVO

	• Bei Unsicherheit hinsichtlich Betroffenheit informieren, Pflicht entfällt nur bei Feststellung der Nichtbetroffenheit (WP 213)
	• Bei Vermutung nachforschen
	  • Übergang von Vermutung zu Kenntnis kritisch
	  • Zeitpunkt dokumentieren
	• Benachrichtigungspflicht entfällt, wenn
	  • Geeignete TOMs vorhanden und angewendet (z. B. Verschlüsselung)
	  • Nachfolgende Maßnahmen zur wahrscheinlichen Vermeidung des hohen Risikos
	  • Unverhältnismäßiger Aufwand => öffentliche Bekanntmachung o. ä.

Technische und organisatorische Maßnahmen <-> Sicherheit der Verarbeitung

Technische und organisatorische Maßnahmen <-> Sicherheit der Verarbeitung

Alte Rechtslage § 9 BDSG	Neue Rechtslage Art. 32 DSGVO
Bei selbstständiger Verarbeitung oder im Auftrag	Verantwortliche und der Auftragsverarbeiter
Technische und organisatorische Maßnahmen um die Ausführungen und Anforderungen des BDSG und der Anlage zu § 9 BDSG zu gewährleisten	Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände, der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen
Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht	Geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten

Technische und organisatorische Maßnahmen<-> Sicherheit der Verarbeitung

Alte Rechtslage § 9 BDSG	Neue Rechtslage Art. 32 DSGVO
• Zutrittskontrolle, • Zugangskontrolle, • Zugriffskontrolle, • Weitergabekontrolle, • Eingabekontrolle, • Auftragskontrolle, • Verfügbarkeitskontrolle und • Trennungsgebot	Unter anderem ist sicherzustellen: • Die Vertraulichkeit, • Integrität, • Verfügbarkeit und • Belastbarkeit der Systeme und Dienste • Die Fähigkeit, die Verfügbarkeit der pbD [...] bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Vorabkontrolle
<->
Datenschutzfolgenabschätzung

Vorabkontrolle <-> Datenschutzfolgenabschätzung

Alte Rechtslage § 4d Abs. 5, 6 BDSG	Neue Rechtslage Art. 35 DGSVO
Vor Beginn der Verarbeitung bei besonderen Risiken für Rechte und Freiheiten der Betroffenen (Art des Verfahrens, Tragweite für den Betroffenen, risikoträchtige Zweckbestimmung, Verwendung neuer Technologien)	Vor Beginn der Verarbeitung, bei voraussichtlich hohem Risiko für Rechte und Freiheiten natürlicher Personen, Abschätzung der Folgen (aufgrund der Art, des Umfangs und der Zwecke der Verarbeitung)
Prüfung der Rechtmäßigkeit der Verarbeitung bei • Verarbeitung besonderer pbD • Bewertung der Persönlichkeit (einschl. Fähigkeiten, Leistung, Verhalten)	Insbesondere bei Nutzung neuer Technologie, aufgrund von Art, Umfang, Umständen, Zwecken der Verarbeitung voraussichtlich hohes Risiko für Rechte + Freiheiten natürlicher Personen (Abs. 3) Insbesondere bei • systematischen und umfassenden Bewertungen persönlicher Aspekte • umfangreicher Verarbeitung besonderer Kategorien • systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

Vorabkontrolle <-> Datenschutzfolgenabschätzung

Alte Rechtslage § 4d Abs. 5, 6 BDSG	Neue Rechtslage Art. 35 DGSVO
Durchzuführen durch betrieblichen oder behördlichen DSB nach Empfang der Verfahrensübersicht	Durchführung durch den Verantwortlichen (DSB ist beratend einzubinden) (Abs. 2)
Prüfung der materiellen Rechtmäßigkeit	Geht über reine Prüfung der Rechtmäßigkeit hinaus
Empfohlener Prüfumfang: Vorhandensein einer RGL, betroffene Personengruppen und Daten(kategorien), Verarbeitungszweck, mögliche Empfänger, TOMs, Grundsätze nach § 3a, Betroffenenrechte, Regelungen zur Transparenz	Mindestumfang (Abs. 7) • Systematische Beschreibung der geplanten Verarbeitungsvorgänge • Zwecke der Verarbeitung • Bewertung der Notwendigkeit und Verhältnismäßigkeit i. H. a. den Zweck

Vorabkontrolle <-> Datenschutzfolgenabschätzung

Alte Rechtslage § 4d Abs. 5, 6 BDSG	Neue Rechtslage Art. 35 DGSVO
	• Bewertung der Risiken für die Rechte und Freiheiten • Zur Bewältigung der Risiken geplante Abhilfemaßnahmen
Stellungnahme des DSB möglichst in schriftlicher Form, ebenso wie für wesentliche Erwägungen	Erstellung eines DSFA-Berichts ... Überwachung und Fortschreibung der DSFA (z. B. bei Änderungen in der Verarbeitung)

Weitere implizite Anforderungen

- **Einwilligung:**
  - Art. 6 Abs.1 lit. a i. V. m. Art. 7 Abs.1 DSGVO
  - „Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, [...].“ Ebenso EG 42
- **Identifizierbarkeit des Betroffenen:**
  - Art. 11 Abs. 2 DSGVO
  - „Kann der Verantwortliche in Fällen gemäß Absatz 1 des vorliegenden Artikels nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, [...].“
- **Widerspruchsrecht:**
  - Art. 21 Abs. 1 DSGVO
  - „ 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, [...].“

Weitere (implizite) Anforderungen

- **Verantwortlichkeit:**
  - Art. 24 Abs. 1 DSGVO
  - „[...] geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. “ Ähnlich EG 74
- **Data Protection by Design and by Default:**
  - Art. 25 DSGVO i. V. m. EG 78
  - „Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen,, [...].“
- **Datenschutzverordnung S.-H. (SDVO):**
  - Bis 31.12.2018 gültig
  - Darüber hinaus wahrscheinlich ähnliche Anforderungen

Weitere Informationen

- https://www.datenschutzzentrum.de/:
  - Muster (u.a. Verzeichnis der Verarbeitungstätigkeiten)
  - Vorlagen Dokumentation nach DSVO
  - Kurzpapiere der Datenschutzkonferenz
  - Gesetze

Vielen Dank!

Noch Fragen?

Christian Prietz
ULD78@datenschutzzentrum.de
Tel. 0431-988 1224

www.datenschutzzentrum.de