Mittelstand 4.0
Kompetenzzentrum
Siegen

Verarbeitungsverzeichnis

Warum?

a) gesetzliche Grundlage

- Artikel 30 DSGVO: Pflicht zur Dokumentation der Datenverarbeitungsprozesse
  - → bisher (in D.) bereits gefordertes Verfahrensverzeichnis (§ 4g Abs. 2 BDSG a.F.) wird nun durch ein Verzeichnis über sämtliche Verarbeitungstätigkeiten ersetzt
  - Tipp: prüfen, ob bereits ein Verzeichnis nach alter Rechtslage geführt wurde und ggf. zur Grundlage des neuen Verzeichnisses machen

b) Zielsetzung

- Übersicht über die datenschutzrelevanten Abläufe im Betrieb
  - Auf Grundlage dessen: für Ausmaß und Intensität der betrieblichen Datenverarbeitung sensibilisieren

c) Verpflichtung

- des Verantwortlichen (Art. 30 Abs. 1 Satz 1 DSGVO)
- des Auftragsverarbeiters (Art. 30 Abs. 2 DSGVO)
- bzw. deren (gesetzliche) Vertreter

- Achtung: Inhaltliche Unterschiede der Verarbeitungsverzeichnisse von Verantwortlichen und Auftragsverarbeiter

- Art. 30 Abs. 5 DSGVO: Ausnahme von der Pflicht zur Erstellung eines Verarbeitungsverzeichnisses für
  - Verantwortliche oder Auftragsverarbeiter, die weniger als 250 Beschäftigte haben,
  - soweit
    - „die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt“
    - oder die Verarbeitung keine besonderen Datenkategorien i.S.d. Art. 9 DSGVO
    - oder strafrechtliche Verurteilungen und Straftaten an sich (Art. 10 DS-GVO) betrifft.

- Form: schriftlich oder elektronisch (Art. 30 Abs. 3 DSGVO)
- ist *der Aufsichtsbehörde auf Nachfrage zur Verfügung zu stellen* (Art. 30 Abs. 4 DSGVO)
- kann ein *Mittel zur Erfüllung der Dokumentationspflichten* nach Art. 24 Abs. 1 DSGVO sein

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Was tun?

- es sind alle Tätigkeiten zu dokumentieren, bei denen personenbezogene Daten verarbeitet werden
    - können in den unterschiedlichsten betrieblichen Situationen vorkommen (z.B. Erstellung und Veränderung der Kundendatei, Verwaltung der Mitarbeiterakten, Verwendung einer Kamera im Betrieb)

Negativ

- Sehr hoher (insb. Initial-)Aufwand (ggf. natürlich auch für Aktualisierungen)
    - Zeit
    - Finanzielle Ressourcen (neue Programme zur Dokumentation; Erweiterung bestehender Tools durch neue Applikationen; ...)
    - Manpower
    - ...

  → erheblich gestiegener Dokumentationsaufwand vor allem für Auftragsverarbeiter (bislang für die im Auftrag verarbeiteten Daten nicht zur Führung verpflichtet, vgl. § 11 Abs. 4 BDSG a.F.)
- immer noch viel Unsicherheit, ob das, was man tut, richtig ist und inwieweit es einen im „Ernstfall“ schützen/helfen kann

- Einwand/Anmerkung:
    - z.T. kann auf „nebenbei entstehende Protokollierung“ zurückgegriffen werden:
        - stark prozess- und serviceorientierte Dienstleistungsunternehmen / solche, die ausschließlich klar definierte Leistungen anbieten (z.B. Cloud Services im Massengeschäft): die erforderlichen Informationen lassen sich meist mit vertretbarem Aufwand auch nachträglich ermitteln
        - heute oft fortgeschrittene Automatisierung von Geschäftsabläufen → viele Nachweispflichten können z.B. durch sowieso stattfindende Protokollierung von Systemvorgängen abgebildet werden

      → Allerdings
        - muss berücksichtigt werden, dass die Umsetzung der prozessualen Einbindung der Dokumentation in die Leistungsbereitstellung nachhaltig geschieht
        - müssen die jeweiligen Anforderungen und der entstehende Anpassungsbedarf früh genug ermittelt und geplant werden
    - Bereits vor Einführung der DSGVO bestand nach alter Rechtslage in D. die Pflicht zur Führung eines Verfahrensverzeichnisses
        - damit ist es keine Aufgabe „von 0 an“ (sollte es zumindest nicht sein)
        - gut geführtes Verfahrensverzeichnis erleichtert erheblich den Übergang vom BDSG zur DSGVO

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Positiv

- Dokumentationen sind nicht allein datenschutzspezifisch:
  - → werden in diversen Vorschriften gefordert
    (Compliance, IT-Sicherheit und ganz aktuell, Geschäftsgeheimnisschutz nur als Beispiele genannt)
  - → mit einer vernünftigen Struktur lassen sich direkt mehrere „Gesetzes-Fliegen“ mit einer Klappe schlagen
- (weniger juristisch als organisatorisch-ökonomisch:) Wissensmanagement als unternehmerisches/wirtschaftliches Problem; Stichworte:
  - Fachkräfte-Mangel
  - Generationenwechsel
  - Transfer
  - Teamwork
  - Einarbeitung
  - ...

  → Gute Prozess-Dokumentationen (also u.a. auch Verarbeitungsverzeichnisse), sind unerlässlich
- Außerdem „Ordnungsfunktion“, aufdecken von:
  - Missständen,
  - ineffizienten Prozessen
  - Entwicklungspotenzialen (für neue Geschäftsfelder?)
  - ...

- Last but not least: dient als Nachweis zur Exkulpation gem. Art. 82 Abs. 3 DSGVO bzw. i.R.d. Meldung der Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde i.S.d. Art. 33 Abs. 1 i.V.m. Erwägungsgrund 86 DSGVO

→ letztlich geht es darum, jemanden, der keine vertieften Kenntnisse von dem konkreten Prozess/der Firma hat (wie es z.B. bei Mitarbeitern der Datenschutzbehörden der Fall wäre), das Verarbeitungsverfahren (inkl. der Verantwortlichkeit, Ziele, Inhalte, Risiken, ...) verständlich aufzuzeigen

→ Wissensmanagement als zusätzlicher „Anreiz“

→ zum Aufwand/Vorgehen: besser peu à peu als gar nicht oder schlecht. Anfangen: am besten mit den kleinsten, unproblematischsten Verarbeitungen, um zu „üben“ oder, wenn besonders ausgeprägtes Risiko, mit denen wo eine Verletzung am wahrscheinlichsten/folgenreichsten wäre

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Wie?

- Inhaltliche Anforderungen
  - Verantwortlicher, gem. Art. 30 Abs. 1 DSGVO:
    - Name und Kontaktdaten des Verantwortlichen (lit. a)
      - sowie ggf. des gemeinsam Verantwortlichen und ggf. des jeweiligen Vertreters (i.S.d. Art. 27 DSGVO)
      - und eines ggf. benannten DSB
    - Zwecke der Verarbeitung (lit. b),
    - Kategorien der betroffenen Personen & der verarbeiteten personenbezogenen Daten (lit. c),
    - Kategorien von Empfängern der personenbezogenen Daten einschließlich Empfängern in Drittstaaten (inkl. internationalen Organisationen) (lit. d),
    - Übermittlung in Drittstaaten (lit. e),
    - „wenn möglich“, Löschfristen (lit. f),
    - „wenn möglich“, eine allgemeine Beschreibung der ergriffenen TOM i.S.d. Art. 32 Abs. 1 DSGVO (lit. g)

  - Auftragsverarbeiter, gem. Art. 30 Abs. 2 DSGVO:
    → etwas geringer als beim Verantwortlichen
    - Namen und Kontaktdaten der beteiligten Auftragsverarbeiter (lit. a)
      - und der beauftragenden Verantwortlichen sowie ggf. von deren Vertretern
      - und eines etwaig benannten DSB
    - Kategorien der Verarbeitungen, die im Auftrag des Verantwortlichen durchzuführen (lit. b)
    - Information über Übermittlungen an ein Drittland oder eine internationale Organisation inklusive ggf. bestehender Garantien i.S.d. Art. 49 Abs. 1 Unterabs. 2 DSGVO (lit c)
    - „wenn möglich“ allgemeine Beschreibung der ergriffenen TOM gem. Art. 32 Abs. 1 DSGVO (lit. d)

→ es gibt kein Patentrezept, nicht genau DAS eine Muster, wie ein Verarbeitungsverzeichnis auszusehen/zu erscheinen hat. Wichtig ist, dass die grundsätzlich erforderlichen Informationen enthält und seinen Zweck (s.o.) erfüllt

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Vorgehen/Aufbau

1. ein einheitliches, schlüssiges System wählen, dass zu den eigenen Anforderungen und Verarbeitungsvorgängen passt (ganz banal z.B.: Papierform oder digital, zentrale Ablage oder in den einzelnen Abteilungen, Verantwortung für Updates?, ...)

2. Formale Voraussetzungen anschauen & umsetzen (also erstmal die Basis-Informationen / das sog. „Stammdatenblatt“)
   → Allgemeine Angaben wie
   - Name und Kontaktdaten des für die Verarbeitung (gemeinsam) Verantwortlichen, ...) / des Betriebs (bei juristischen Personen zudem Name des Vertreters, z.B. Name des Geschäftsführers)
   - Name und Kontaktdaten des Datenschutzbeauftragten, falls bestellt

3. Analyse der einzelnen Datenverarbeitungsvorgänge/Zusammenfassung verschiedener Datenverarbeitungen zu einem zu dokumentierenden Prozess
   [Bsp.: Empfang an der Unternehmenszentrale: entweder Verarbeitungsvorgang „Telefongespräche“ und dann aufgliedern in unterschiedliche Anlässe für Telefonate, oder Verarbeitungsvorgang „Terminvergabe“ untergliedern in persönlich/telefonisch/online/...]

4. Zwecke und Beschreibung der Datenverarbeitung / Detailangaben zu den einzelnen Datenverarbeitungszwecken; folgende Pflichtangaben – vgl. Art. 30:
   a. Kategorien der betroffenen Personen
      [*Beschreibung der Kategorien betroffener Personen (zB Kunden, Mitarbeiter, Lieferanten usw.)]*
   b. Zwecke der Verarbeitung (z.B. für Werbemaßnahmen oder zur Abwicklung eines Vertrags) und Nennung der Rechtsgrundlagen
      i. Art. 6 DSGVO – einzelne Rechtfertigungsgründe
      ii. Optional/ergänzend: Notiz, wo Verträge, Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten) abgelegt sind
   c. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen
      i. Kategorien der verarbeiteten Daten
      ii. Löschungs- und Aufbewahrungsfristen (wenn möglich)
      [z.B.: „Aufgrund der gesetzlichen Aufbewahrungsfristen auf jeden Fall 7 Jahre; darüber hinaus bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen“ oder „bis zur Beendigung der Geschäftsbeziehungen“] → In der Regel gilt, dass Daten zu löschen sind, wenn sie für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden
   d. Kategorien von Empfängern, an welche personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

i. Kategorien der Empfänger
[z.B. Banken, juristische Vertretung, Behörden, Vertragspartner, Dienstleister, ...]
ii. Übermittlungsort
[Drittstaat, Internationale Organisation – z.B. UNO, OSZE]
iii. Dokumentation der geeigneten Garantien (im Falle einer Übermittlung in Drittstaaten, die nicht auf Art. 45, 46, 47 oder 49 Abs. 1 Unterabs. 1 DSGVO erfolgt)
[v.a., wenn:
- *kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt,*
- *keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden,*
- *keine Corporate Binding Rules zur Anwendung kommen,*
- *die Übermittlung nicht für die Vertragserfüllung erforderlich ist*
- *keine ausdrückliche Einwilligung vorliegt]*

5. Dokumentation der (vor Beginn der Verarbeitung erfolgten!) Datenschutz-Folgenabschätzung bzw. Begründung, wieso nicht durchgeführt

   die Datenschutz-Folgenabschätzung kann sehr gut aus dem Verarbeitungsverzeichnis abgeleitet werden (vgl. Erwägungsgrund 76 DSGVO)
   → Anhand einzelner Verarbeitungstatbestände, wie sie in dem Verzeichnis aufgelistet werden müssen, kann konkret das jeweilige Risiko für die Rechte der Betroffenen analysiert werden
   → Verbindung zwischen Verarbeitungsverzeichnis und Datenschutz-Folgenabschätzung empfiehlt sich daher (auch vor dem Hintergrund regelmäßiger Aktualisierungen)
   → Empfehlung: auf Grundlage des Verarbeitungsverzeichnisses eine konzernweit vereinheitlichte Vorlage für die Durchführung der Datenschutz--Folgenabschätzung zu formulieren

6. Beschreibung der technischen und organisatorischen Maßnahmen (TOM) [„wenn möglich“]
   → Art. 32 DSGVO: Betriebe sind verpflichtet, Maßnahmen auf dem Stand der Technik zu ergreifen, um den Risiken der Datenverarbeitung zu begegnen
   → konkrete Maßnahmen sind nach Einzelfall und Risikobehaftung der Datenverarbeitung zu entscheiden
   → thematische Zusammenfassung auf folgende Kernmaßnahmen (Übergänge sind aber z.T. fließend):

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

1) Vertraulichkeit der Datenverarbeitung
   = Geeignete Maßnahmen, um Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren (u.a. Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle)
   - Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen (z.B.: Schlüsselsysteme, Portier/ Sicherheitspersonal, Alarm- und Videoanlagen)
   - Zugangskontrolle: Schutz vor unbefugter Systembenutzung (z.B.: Passwort-Policy, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern)
   - Zugriffskontrolle: Verhinderung unbefugter Nutzung (Lesen, Kopieren, Verändern oder Entfernen) des Systems (z.B.: Protokollierung von Zugriffen; oder Zugriff nur für konkrete Nutzergruppen)
2) Integrität der Datenverarbeitung
   = Maßnahmen zur Gewährleistung der nachträglichen Überprüfung hinsichtlich des ob/von wem der Eingabe/Veränderung/Entfernung personenbezogener Daten in Datenverarbeitungssystemen (u.a. Eingabekontrolle/ Verarbeitungskontrolle; z.B. Verwendung individueller Benutzernamen)
3) Verfügbarkeitskontrolle
   - Schutzmaßnahmen gegen zufällige Zerstörung/Verlust und Sicherungsmaßnahmen zur Wiederherstellung im Störfall (z.B.: Überwachung von Temperatur und Feuchtigkeit in Serverräumen, Backup-Strategie, Virenschutz, Firewall)
4) Trennungsgebot
   - Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (z.B.: Trennung von Daten verschiedener Auftraggeber, Trennung nach Verarbeitungszwecken)
5) Pseudonymisierung und Verschlüsselung:
   - Pseudonymisierung: Abtrennung (gesonderte Aufbewahrung) primärer Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung
   - Verschlüsselung: Einsatz verschiedener Verschlüsselungstechnologien
6) Evaluierungsmaßnahmen:
   - Datenschutz-Management (zB Risikoanalyse, Datenschutz-Folgenabschätzung), einschließlich regelmäßiger Mitarbeiter-Schulungen

→ dementsprechend sollen die nach Maßgabe u.a. der Risikofolgenabschätzung gewählten TOM aufgelistet werden

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages