Die Umsetzung der DSGVO – rechtliche und technisch-organisatorische Anforderungen

Udo Höhn

Me

- Systemadministrator beim Polizeipräsidium München
- Vom 01.04.1990 bis 31.12.2018 Referent beim Bayer. Landesbeauftragten für den Datenschutz – im Referat Technik und Organisation
- Dozent und Referent bei verschiedenen staatlichen und nicht-staatlichen Einrichtungen
- Herausgeber und Autor zahlreicher Fachpublikationen

Datenschutzreform 2018

- Ab 25.Mai 2018 wurde die **EU-Datenschutz-Grundverordnung (DSGVO)** unmittelbar in jedem Mitgliedstaat wirksam.
- Die DSGVO soll zu einer **Vollharmonisierung** des Datenschutzrechts in Europa führen.
- Die DSGVO hat **Anwendungsvorrang** gegenüber nationalen Recht.
- Nationales Recht (z. B. BDSG und BayDSG) musste daher **angepasst** werden.
- Durch Öffnungs- und Spezifizierungsklauseln haben die nationalen Gesetzgeber v.a. für den öffentlichen Bereich **Gestaltungsspielräume**.

Themenübersicht

- Rechtmäßigkeit der Verarbeitung
- Verarbeitung besonderer Kategorien pers. Daten
- Betroffenenrechte
- Datenschutzmanagement
- Sicherheit der Verarbeitung
- Datenschutz-Folgenabschätzung
- Verzeichnis der Verarbeitungstätigkeiten
- Auftragsverarbeitung
- Meldung von Sicherheitsvorfällen
- Benennung eines Datenschutzbeauftragten

Grundsatz der Rechtmäßigkeit (Art. 5 Abs. 1 a, 1. Fall)

- Die Verarbeitung personenbezogener Daten ist verboten, sofern nicht eine Rechtsvorschrift diese Verarbeitung erlaubt oder die betroffene Person eingewilligt hat.
- Die gesetzlich normierten Erlaubnisse finden sich insbesondere in den Art. 6 (Rechtmäßigkeit der Verarbeitung) und 9 (Verarbeitung besonderer Kategorien personenbezogener Daten).

Zulässigkeit der Verarbeitung

- Erlaubnistatbestände (u.a.):
  - Einwilligung (Art. 6 Abs. 1 Buchst. a DSGVO)
  - Verarbeitung, um eine Aufgabe wahrzunehmen, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (Art. 6 Abs. 1 Buchst. e DSGVO)
    - Keine Generalklausel
    - Verarbeitung n u r in Verbindung mit den jeweiligen Rechtsgrundlagen (Fachrecht oder Art. 4 Abs. 1 BayDSG bzw. § 3 BDSG)

Personenbezogene Daten

Einzelangaben über

- persönliche oder
  - z. B. Angaben zum Namen, Adresse, Familienstand, Kinder, Geburtsdatum, Künstler- oder Deckname, Gesundheitszustand, Konfession, Körpergröße, Alter, Gewicht, Beruf, IP-Adresse, Online-Kennung
- sachliche Verhältnisse
  - beispielsweise Angaben zum Einkommen, Vermögen, Eigentum, Besteuerungsmerkmale, Versicherungen, Verträge
- einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)

Betroffener kann nur eine noch lebende natürliche Person sein.

Verarbeitung

- Der Verarbeitungsbegriff (Art. 4 Nr. 2) der Datenschutz-Grundverordnung umfasst grundsätzlich jeden Verarbeitungsvorgang im Zusammenhang mit personenbezogenen Daten einschließlich deren Erhebung. Die bislang im deutschen Datenschutzrecht gebräuchliche Begriffe „Erhebung, Verarbeitung und Nutzung“ werden durch den einheitlichen Begriff der Verarbeitung ersetzt.
- Die Verarbeitung kann sowohl automatisiert als auch nicht-automatisiert erfolgen.

Einwilligung I (Art. 7)

- Verantwortlicher muss die Einwilligung nachweisen können
- Einwilligung muss
  - durch eine eindeutige bestätigende Handlung erfolgen,
  - mit der freiwillig,
  - für den konkreten Fall,
  - in informierter Weise und
  - unmissverständlich das Einverständnis bekundet wird.
- Form:
  - Schriftlich, elektronisch (z. B. durch Anklicken eines Kästchens), mündlich oder andere Verhaltensweise
  - Vorformulierung muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache gehalten sein

Einwilligung II (Art. 7)

- Einwilligung kann jederzeit widerrufen werden (Art. 7 Abs. 3 DSGVO)
- Nachweispflicht (Art. 7 Abs. 1 DSGVO)
- Praxisfragen
  - Fortgeltung bisher erteilter Einwilligungen: ErwGr 171 Satz 3 DSGVO; ErwGr 32 DSGVO
  - Abwägung: Einwilligung gegenüber anderen Verarbeitungsbefugnissen
  - Vorgehensweise, insbesondere bei elektronisch erteilter Einwilligung (z. B. durch Anklicken eines Kästchens)

Nationale Rechtsgrundlage: Art. 4 Abs. 1 BayDSG

- Art. 4 Abs. 1 BayDSG 2018 ist eine Rechtsgrundlage im Sinne von Art. 6 Abs. 1 Buchst. e, Abs. 3 Satz 1 Buchst. b DSGVO
- Art. 4 Abs. 1 BayDSG 2018:
  „Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung einer ihr obliegenden Aufgabe erforderlich ist.“
- Öffentliche Stellen als Wettbewerbsunternehmen im Sinne von Art. 1 Abs. 3 Satz 1 BayDSG: Anwendung des BDSG (Aufsicht aber durch den BayLfD)

Zweckbindungsgrundsatz (Art. 5 Abs. 1 b)

- Personenbezogene Daten dürfen grundsätzlich nur für den Zweck verwendet werden, für den sie erhoben worden sind.
- Die Zwecke der Datenverarbeitung müssen somit bereits bei der Erhebung personenbezogener Daten festgelegt, nicht zu allgemein gehalten und legitim sein.
- Eine Weiterverarbeitung der Daten ist unzulässig, wenn sie mit diesen Erhebungszwecken nicht zu vereinbaren ist.

Verarbeitung besond. Kategorien pers. Daten (Art. 9 Abs. 1)

Die Verarbeitung ist bei folgenden personenbezogener Daten generell untersagt:

- rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,
- Gewerkschaftszugehörigkeit
- genetische Daten,
- biometrischen Daten,
- Gesundheitsdaten oder
- Daten zum Sexualleben oder der sexuellen Orientierung

Ausnahmen (Art. 9 Abs. 2)

- Betroffener hat eingewilligt
- zur Ausübung der Rechte und Pflichten aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes
- zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person
- Daten, die die betroffene Person offensichtlich öffentlich gemacht hat
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit usw.
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit

Grundsatz der Verantwortlichkeit (Art. 5 Abs. 2)

- Die Einhaltung der dargestellten Grundsätze ist durch den Verantwortlichen nachzuweisen (sog. **Rechenschaftspflicht**), z. B.
  - Anforderungen der Rechtmäßigkeit und der Transparenz der Datenverarbeitung sowie
  - Verarbeitung der Daten nach Treu und Glauben,
  - Beachtung des Zweckbindungsgrundsatzes, des Grundsatzes der Datenminimierung, der Richtigkeit der Daten, der Speicherbegrenzung und der Integrität und Vertraulichkeit der Datenverarbeitung.
- Aufsichtsbehörde kann vom Verantwortlichen die Herausgabe seiner Dokumentation fordern

Verantwortlicher

- „Verantwortlicher“ ist nach Art. 4 Nr. 7 DSGVO „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“.
- Nach Art. 3 Abs.2 BayDSG ist Verantwortlicher im Sinne der DSGVO „die für die Verarbeitung zuständige öffentliche Stelle“
- Verantwortlicher = Behörde (und damit **vorrangig der Behördenleiter**)
- Wer die vielfältigen Pflichten des Verantwortlichen in der öffentlichen Stelle konkret erfüllt, ist intern festzulegen.

Betroffenenrechte

- Informationspflicht
- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung/Vergessenwerden
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenportabilität
- Widerspruchsrecht
- Einschränkung durch
  - Fachgesetze (z. B. Art. 27 BayKrG)
  - BayDSG (z.B. Art. 10 Abs. 2, 26 Abs. 3 ff. BayDSG)

Auskunftsrecht (Art. 15)

- Auskunft auf Verlangen
- Auskunftsumfang (z. B. über Verarbeitungszwecke, Kategorien personenbezogener Daten, Empfänger oder Kategorien von Empfängern, geplante Dauer der Speicherung, Bestehen eines Rechts auf Berichtigung oder Löschung der Daten, Beschwerderecht, Herkunft der Daten)
- Recht auf Erstellung und Erhalt einer Kopie der personenbezogenen Daten
- Modalitäten (Form, Kostenfreiheit, Ausnahme: Rechte und Freiheiten anderer Personen)

Recht auf Berichtigung (Art. 16) / Recht auf Löschung (Art. 17)

- Berichtigung bei Unrichtigkeit
- Löschungsgründe
  - Unzulässige Speicherung
  - Sensible personenbezogene Daten (§ 3 Abs. 9 BDSG), wenn die Richtigkeit nicht bewiesen werden kann
  - Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich
- Recht auf „Vergessenwerden“
  - Diejenigen, die personenbezogene Daten erhoben haben, müssen diese „vergessen” (löschen), wenn die gesetzlichen Voraussetzung dafür vorliegen. Wer die Daten verwendet hat, muss auch sicherstellen, dass jede Kopie dieser Daten im Internet und jeder Link darauf gelöscht wird (Art. 17 Abs. 2).

Einschränkung der Verarbeitung

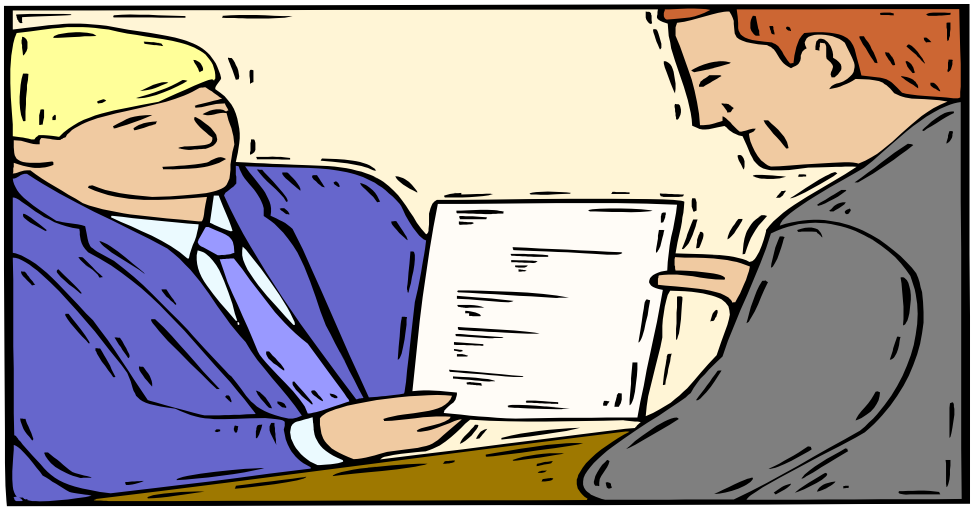
- Einschränkung der Verarbeitung
  - Ein Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO besteht zum Beispiel dann, wenn der Verantwortliche die Daten nicht mehr länger, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt oder die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat und noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Recht auf Datenportabilität / Widerspruchsrecht

- Recht auf Datenportabilität
  - In Artikel 20 DSGVO wird das Recht des Betroffenen auf Datenportabilität (Mitnahme seiner Daten durch den Betroffenen) eingeführt, d. h. das Recht, seine Daten aus einem automatisierten Datenverarbeitungssystem auf ein anderes System zu übertragen, ohne dass der für die Verarbeitung Verantwortliche ihn daran hindern kann.
- Widerspruchsrecht (Art. 21 DSGVO)
  - Erfolgt eine Datenverarbeitung durch den Verantwortlichen ohne Einwilligung aufgrund der gesetzesmäßigen Wahrnehmung berechtigter Interessen, so steht dem Betroffenen das Recht zu, dieser Verarbeitung zu widersprechen.

Datenschutzmanagement (Teil 1)

- Gesetzliche Verpflichtung (Art. 32 Abs. 1 Buchstabe d DSGVO)
- Begriff
  - Managementmethode, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, zu organisieren, zu steuern und zu kontrollieren
- Umsetzung
  - Datenschutzkonzept



Datenschutzmanagement (Teil 2)

- Einhaltung von Standards
  - z. B. IT-Grundschutzkataloge
- Aufrechterhaltung des Datenschutzes im laufenden Betrieb (Berücksichtigung von Änderungen und Störungen)
  - Änderungen im Datenschutzrecht
  - Änderungen in den (IT-)Verfahren
  - Störungen in den operativen Betriebsabläufen, die als Sicherheitsvorfall zu klassifizieren sind
  - Technischer Fortschritt und reduzierter Aufwand für bisher nicht realisierte Maßnahmen

Datenschutzmanagement (Teil 3)

- Überprüfung des Datenschutzmanagementsystems
- zu beachtende gesetzliche Regelungen:
  - Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO)
  - Rechte der betroffenen Person (Art. 12 – 23 DSGVO)
  - Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)
  - Sicherheit der Verarbeitung (Art. 32 DSGVO)
  - Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 Abs. 1 DSGVO)
  - Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Art. 34 Abs. 1 DSGVO)
  - Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

Datenschutzmanagement (Teil 4)

- Beispiel für Inhalte:
  - Bestimmung eines behördlichen Datenschutzbeauftragten (und eines Vertreters)
  - Aufgabenbeschreibung des behördlichen DSB
  - Definition und Umsetzung von technisch-organisatorischen Maßnahmen
  - Wer meldet Datenpannen? (Vertretungsbedarf)
  - Vorgaben für die Auftragsverarbeitung
  - Wer führt das Verzeichnis von Verarbeitungstätigkeiten und in welcher Form
  - Regelungen für die Durchführung von Datenschutz-Folgenabschätzung usw.

Sicherheit der Verarbeitung (Art. 32 Abs. 1)

- Es müssen technische und organisatorische Maßnahmen ergriffen werden unter Berücksichtigung
  - des Stands der Technik
  - der Implementierungskosten
  - der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
  - Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen
- Beispiele
  - Pseudonymisierung und Verschlüsselung (Datenübertragung, Personaldaten)
  - Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme

Vertraulichkeit

- Schutz vor unbefugter Kenntnisnahme der Daten
- Maßnahmen:
  - Zugangs- und Zugriffskontrolle
  - Starke Verschlüsselung bei Datenspeicherung und Datenübermittlung
  - Revisionsfähige Rechtevergabe
  - Restriktive Vergabe von Zugriffsrechten
  - Anonymisierung bzw. Pseudonymisierung
  - Verbot des Einsatzes privater Hard- und Software
  - Datenschutzgerechte Entsorgung von Datenträgern

Integrität

- Gewährleistung der
  - Echtheit, Vollständigkeit
  - Zurechenbarkeit, Urheberschaft
  - (Rechts-)Gültigkeit
- Maßnahmen:
  - Einsatz der elektronischen Signatur
  - Protokollierung von Datenänderungen
  - Kontrolle der Durchführung von Wartung oder Fernwartung
  - Einsatz von Schadensbekämpfungssoftware
  - Einsatz von Firewalls

Verfügbarkeit

- Dienstleistungen, IT-Funktionen, Netzen, Anwendungen oder Informationen müssen stets wie gewünscht zur Verfügung stehen.
- Von jeder Behörde muss geklärt werden, wie lange maximal auf den Rechner bzw. dem Zugriff auf die gespeicherten Daten verzichtet werden kann.
  - Erstellung eines Notfallkonzepts
- Verletzung der Verfügbarkeit
  - Informationen gehen verloren bzw. sind logisch nicht mehr zugreifbar

Belastbarkeit

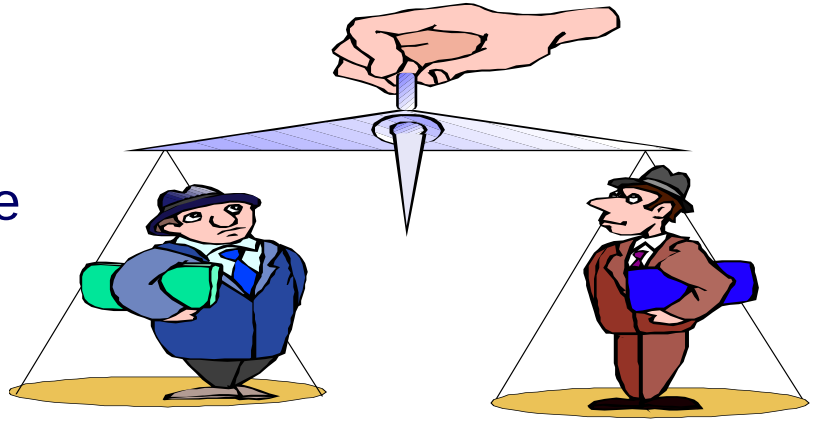
- Datenschutzgrundverordnung enthält keine näheren Angaben bezüglich der Gewährleistung der Belastbarkeit der Systeme und Dienste
- Vermutlich Abzielung auf die Widerstandsfähigkeit der Systeme und Dienste
  - müssen einer gewissen Beanspruchung standhalten können, ohne das es zu einer Überlastung oder Ausfall kommt

Datenschutz-Folgenabschätzung (Teil 1)

- Begriff
  - Instrument, um das Risiko zu erkennen und zu bewerten, das für das Individuum in dessen unterschiedlichen Rollen (als Bürger, Kunde, Patient etc.) durch den Einsatz einer bestimmten Technologie oder eines Systems durch eine Organisation entsteht
- Gesetzliche Pflicht (Art. 35 Abs. 1 DSGVO)
  - Verwendung neuer Technologien
  - Bestehen eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen
  - Einbindung des Datenschutzbeauftragten

Datenschutz-Folgenabschätzung (Teil 2)

- Fallgruppen (Art. 35 Abs. 3 DSGVO)
  - systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen (z. B. Profiling, Scoring)
  - **umfangreiche** Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1
  - systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (z. B. mittels Videoüberwachung)
- Aufsichtsbehörden müssen Listen erstellen (Art. 35 Abs. 4 DSGVO)
  - Positivliste
  - Negativliste



Datenschutz-Folgenabschätzung (Teil 3)

- Mindestanforderungen (Art. 35 Abs. 7 DSGVO)
  - systematische Beschreibung der geplanten Verarbeitungsvorgänge und Zwecke der Verarbeitung
  - Bewertung der Notwendigkeit/Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
  - Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
  - geplante Sicherheitsmaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die DSGVO eingehalten wird

Datenschutz-Folgenabschätzung (Teil 4)

- Einhaltung genehmigter Verhaltensregeln
  (Verbände und Vereinigungen, die Kategorien von Verantwortlichen vertreten – müssen Aufsichtsbehörde vorgelegt werden)
- Einbindung der Betroffenen
  - Gegebenenfalls, also ausnahmsweise oder wo es zweckmäßig erscheint
- Ausnahmen
  - Verarbeitungsvorgänge, die entweder zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe erforderlich sind, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt
  - Datenschutz-Folgenabschätzung wurde bereits vom fachlich zuständigen Staatsministerium durchgeführt oder von einer anderen öffentliche Stelle und wird unverändert übernommen

Datenschutz-Folgenabschätzung (Teil 5)

- Erneute Datenschutz-Folgenabschätzung (Art. 35 Abs. 11 DSGVO)
  - bei wesentlichen Verfahrensänderungen, neuen Risiken etc.
- vorherige Konsultation der Aufsichtsbehörden (Art. 36 Abs. 1, 3 DSGVO) bei hohem Risiko
  - Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen
  - Zwecke und Mittel der beabsichtigten Verarbeitung
  - zum Schutz der Rechte und Freiheiten der betroffenen Personen vorgesehenen Maßnahmen und Garantien
  - Kontaktdaten des Datenschutzbeauftragten
  - alle sonstigen von der Aufsichtsbehörde angeforderten Informationen

Verzeichnis der Verarbeitungstätigkeiten (1)

- Wozu?
  - trägt zur Erfüllung der Dokumentationspflicht (Art. 5 Abs. 2 DSGVO) bei
  - ist Anknüpfungspunkt für Betroffenenrechte (Art. 12 ff. DSGVO)
- Weiterentwicklung des bisherigen Verfahrensverzeichnisses
  - Identifizierung und Einpflegen zusätzlich erforderlicher Angaben bei den bereits erfassten Verfahren
  - Identifizierung und Einpflegen zusätzlich aufzunehmender Verfahren (auch nicht automatisierte Verarbeitungstätigkeiten sind aufzunehmen)

Verzeichnis der Verarbeitungstätigkeiten (2)

- Erforderliche Angaben (Verantwortlicher – Art. 30 Abs. 1 Satz 2 DSGVO)
  - Namen und Kontaktdaten des Verantwortlichen, des Vertreters sowie des Datenschutzbeauftragten
  - Zwecke und Rechtsgrundlage der Verarbeitung
  - Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
  - Kategorien von Empfängern und Rechtsgrundlage
  - Übermittlungen von personenbezogenen Daten an ein Drittland
  - Fristen für die Löschung der Datenkategorien
  - Beschreibung der technischen und organisatorischen Maßnahmen

Verzeichnis der Verarbeitungstätigkeiten (3)

- Formvorschrift (Art. 30 Abs. 3 DSGVO)
  - schriftlich
  - elektronisches Format
- Einsichtsrecht der Aufsichtsbehörde (Art. 30 Abs. 4 DSGVO)
- Ausnahme bei Unternehmen, aber nicht bei Behörden
  - weniger als 250 Mitarbeiter
  - kein Risiko für die Rechte und Freiheiten Betroffener
  - Verarbeitung nicht nur gelegentlich
  - keine Verarbeitung besonderer Datenkategorien

Auftragsverarbeitung (1)

- **Verantwortlicher**
  - Adressat der Betroffenenrechte
  - Weisungsbefugnis
- **Haftung**
  - Grundsätzlich haften sowohl der Verantwortliche als auch der Auftragsverarbeiter
  - Der Auftragsverarbeiter aber nur bei Verstoß gegen die ihm aufgrund der DSGVO auferlegten Pflichten oder bei Nichtbeachtung einer Weisung
  - Rückgriffverfahren gegen Vertragspartner

Auftragsverarbeitung (2)

- **Sicherheitsmaßnahmen**
  - Festlegung der Sicherheitsmaßnahmen
  - Pseudonymisierung, Verschlüsselung
  - Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste
  - Überprüfung, Bewertung und Evaluierung der Wirksamkeit der t-o Maßnahmen
  - Überprüfung der Effektivität der Maßnahmen
  - evtl. Datenschutz-Folgeabschätzung
  - Zertifizierungsverfahren kann als Nachwies dienen

Auftragsverarbeitung (3)

- **Auswahlkriterien**
  - Verarbeitung muss im Einklang mit den Anforderungen der Datenschutzgrund-Verordnung erfolgen
  - Datensicherheitskonzept
  - Datenschutzaudit oder Datenschutzgütesiegel
  - Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens
  - Erkundigung bei Fachverbänden oder anderen Unternehmen
  - Kostenfrage

Auftragsverarbeitung (4)

- **Weiterer Verarbeiter**
  - vorherige Genehmigung durch den Verantwortlichen
  - Informierung über jede beabsichtigte Änderung
  - Einspruch- und Untersagungsrecht des Verantwortlichen
  - Auferlegung von Datenschutzpflichten
  - Haftung durch ersten Auftragsverarbeiter

Auftragsverarbeitung (5)

- **Vertragsgestaltung (1)**
  - Schriftlich (auch elektronisches Format möglich)
  - Gegenstand und Dauer der Verarbeitung
  - Art und Zweck der Verarbeitung
  - Art der personenbezogenen Daten
  - Kategorien betroffener Personen
  - Pflichten und Rechte des Verantwortlichen
  - Dokumentierte Weisung
  - Verpflichtung zur Vertraulichkeit
  - Ergreifung der erforderlichen Sicherheitsmaßnahmen
  - Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters

Auftragsverarbeitung (6)

- **Vertragsgestaltung (2)**
  - Unterstützungspflicht bezüglich der Ergreifung von geeigneten technischen und organisatorischen Maßnahmen
  - Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten
  - Löschung oder Rückgabe aller personenbezogenen Daten nach Vertragsende
  - Zurverfügungstellung der erforderlichen Informationen
  - Überprüfungen — einschließlich Inspektionen – durch den Verantwortlichen möglich
  - Hinweispflicht auf Datenschutzverstöße

Auftragsverarbeitung (7)

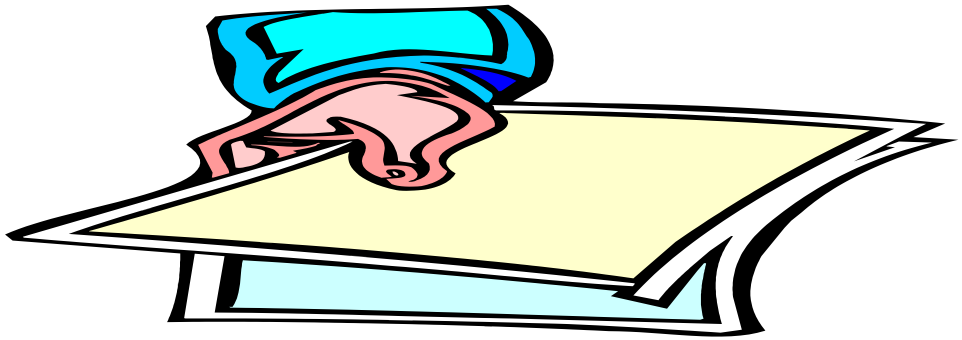
- **Vertragsgestaltung (3)**
  - Detaillierte Aufführung der erforderlichen Sicherheitsmaßnahmen (z. B. physikalischer Schutz der genutzten Server und Serverräume, revisionsfähige Berechtigungsvergabe, Maßnahmen im Katastrophenfall und Maßnahmen zur Gewährleistung der Revisionsfähigkeit)
  - Weitere Angaben (Realisierungszeitraum, Umfang der Datenerhebung, -verarbeitung oder -nutzung, Berichtigung, Löschung und Sperrung von Daten, Zeitpunkt und Art der Löschung bzw. Vernichtung von Datenträgern. Versendungs- und Aufbewahrungsrichtlinien für Datenträger, Festlegung der Örtlichkeit der Datenverarbeitung usw.)

Auftragsverarbeitung (8)

- **Dokumentationspflicht des Verantwortlichen (1)**
  - Bestandteil des zu führenden Verzeichnisses der Verarbeitungstätigkeiten
  - Name und Kontaktdaten des Verantwortlichen, Vertreter des Verantwortlichen sowie des Datenschutzbeauftragten, Zwecke der Verarbeitung, Beschreibung der Kategorien betroffener Personen und der personenbezogenen Daten, Empfänger, gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland, vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien, allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Auftragsverarbeitung (9)

- **Dokumentationspflicht des Verantwortlichen (2)**
  - Schriftlich (auch in elektronischer Form möglich)
  - Weitergabe an die Aufsichtsbehörde auf Anfrage
- **Überwachung des Auftragsverarbeiters durch den Verantwortlichen**



Auftragsverarbeitung (10)

- **Rolle der Aufsichtsbehörde (1)**
  - Kontroll- und Bußgeldbehörde
    - Pflicht zur Bereitstellung von Informationen durch den Verantwortlichen und den Auftragsverarbeiter
    - Hinweise auf eventuelle Datenschutzverstöße
    - Zugangsrecht zu allen erforderlichen personenbezogenen Daten und Informationen, Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte
    - Abhilfebefugnisse
    - Verhängung von Geldbußen

Auftragsverarbeitung (11)

- **Rolle der Aufsichtsbehörde (2)**
  - Erstellung von Standardverträgen
    - Gültigkeit in der gesamten EU
    - Verantwortliche und Auftragsverarbeiter können entscheiden, ob sie lieber einen individuellen Vertrag oder derartige Standardvertragsklauseln verwenden
  - Zusammenarbeit mit dem Verantwortlichen und Auftragsverarbeiter
    - Sensibilisierung und Beratung der Verantwortlichen und Auftragsverarbeiter
  - Zertifizierung
    - Nachweis zur Erfüllung der Pflichten des Verantwortlichen
    - Freiwilligkeit

Meldung von Sicherheitsvorfällen (Teil 1)

- Meldung an die Aufsichtsbehörde
  - Bei Verletzung des Schutzes personenbezogener Daten
  - Unverzüglich und möglichst binnen 72 Stunden
  - Ausnahme: Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen
- Inhalt der Meldung
  - Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten
  - Name und Kontaktdaten des Datenschutzbeauftragten
  - Beschreibung der wahrscheinlichen Verletzungsfolgen
  - Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen

Meldeformular des BayLfD

DER BAYERISCHE LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

Art der Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 3 Buchst. a DSGVO)

- [ ] Gerät verloren
- [ ] Unterlagen verloren oder an einem unsicheren Platz gelagert
- [ ] Unverschlüsselter E-Mail-Versand (besondere Kategorien personenbezogener Daten (Art. 9 DSGVO))
- [ ] Unverschlüsselter E-Mail-Versand (Steuer- oder Sozialdaten)
- [ ] Postsendung ging verloren oder wurde versehentlich geöffnet
- [ ] Hackerangriff, Schadsoftware, Phishing
- [x] Nicht datenschutzgerechte Entsorgung von Materialien (z. B. Akten, Bild- oder Tonträger)
- [ ] Nicht datenschutzgerechte Geräteentsorgung (z.B. Festplatten)
- [ ] Missbrauch von Zugriffsrechten (Nichtberechtigter Abruf durch eigene Mitarbeiter)
- [ ] Unbeabsichtigte Veröffentlichung
- [ ] Webportal zeigte falsche / fremde Daten an
- [ ] Personenbezogene Daten an falschen Empfänger gesendet
- [ ] Sonstiges

Meldung von Sicherheitsvorfällen (Teil 2)

- Benachrichtigung des Betroffenen
  - bei hohem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen (Art. 34 Abs. 1 DSGVO)
  - keine Benachrichtigung erforderlich (Art. 34 Abs. 3)
    - Verantwortliche hat geeignete technische und organisatorische getroffen, um einen unerlaubten Zugriff zu verhindern
    - Verantwortliche hat sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen nicht mehr besteht,
    - Falls dies mit einem unverhältnismäßigen Aufwand verbunden wäre (stattdessen öffentliche Bekanntmachung)
  - Aufforderung durch die Aufsichtsbehörde
- Dokumentation von Sicherheitsvorfällen

Datenschutzbeauftragter

- Verantwortlichkeiten
- Bestellungsvoraussetzungen
- Persönliche Voraussetzungen
- Rechtsstellung
- Befugnisse und Pflichten
- Aufgaben

Verantwortlichkeiten

- Verantwortlicher
- Unterstützung und Beratung durch DSB
- Eigene Verantwortlichkeit der Mitarbeiter
  - Gewährleistung Datenschutz/-sicherheit
- Auftragsverarbeitung

Bestellungsvoraussetzungen

- Jede öffentlichen Stelle, die personenbezogene Daten mittels automatisierter Verfahren verarbeitet o. nutzt, muss einen behördlichen Datenschutzbeauftragter benennen (Art. 37 Abs. 1 Buchstabe a DSGVO).
- Formvorschriften
  - keine schriftliche Bestellung erforderlich
  - Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten und Mitteilung dieser Daten an die Aufsichtsbehörde
  - kein Mitbestimmungsrecht des Personalrats
- Neubenennung (bzgl. eines bisherigen DSB) nicht nötig

Gemeinsamer/externer Datenschutzbeauftragter

- Gemeinsamer Datenschutzbeauftragte mehrerer Behörden oder öffentliche Stellen (Art. 37 Abs. 3 DSGVO)
- Bestellung durch höhere Behörde möglich (nur bei Staatsbehörden – Art. 12 Abs. 3 BayDSG)
- Externer Datenschutzbeauftragter (Art. 37 Abs. 6 DS-GVO)
  - auf Grundlage eines Dienstleistungsvertrags
  - Sofern dafür eine Qualifikation besteht
  - Verpflichtung nach § 1 Abs. 1 Nr. 1 Verpflichtungsgesetz
  - Zeugnisverweigerungsrecht wie Mitarbeiter der öffentl. Stelle
  - Kontrollrechte umfassen auch personenbezogene Daten, die einem Amts- oder Berufsgeheimnis unterliegen

Persönliche Voraussetzungen (1)

- berufliche Qualifikation erforderlich (Art. 37 Abs. 5 DSGVO)
  - Erfahrung sowohl im einzelstaatlichen als auch im europäischen Datenschutzrecht und in der diesbezüglichen Praxis
  - umfassendes Verständnis der Datenschutz-Grundverordnung, des BayDSG und anderer Datenschutzvorschriften
  - fundierte Kenntnis behördlicher Verwaltungsvorschriften

Persönliche Voraussetzungen (2)

- Fachkunde (fundierte Datenschutz- und allgemeine Rechtskenntnisse, EDV-Kenntnisse)
  - Kenntnisse erforderlich über
    - Geschäftszweck, Aufgaben und Struktur der verantwortlichen Stelle
    - die eingesetzten DV-Systeme und -Verfahren (z. B. Betriebssysteme, Standard- und anwendungsbezogene Software)
    - datenschutzrechtliche Kenntnisse allgemein und im Besonderen für die Tätigkeit des Unternehmens
    - die Fachkunde kann grundsätzlich nur durch Teilnahme an entsprechenden Seminaren erworben werden
    - zusätzlich ist das Lesen von Fachliteratur erforderlich
    - Pflicht zur Weiterbildung

Persönliche Voraussetzungen (3)

- Fähigkeit zur Erfüllung seiner Aufgaben
  - persönliche Eigenschaften und Kenntnisse
  - Position innerhalb der Einrichtung
- Interessenkollision (Art. 38 Abs. 6 DSGVO)
  - Verantwortlicher,
  - Leiter der IT-Stelle,
  - Systemverwalter,
  - Leiter der Personalstelle etc.

scheiden aus

Persönliche Stellung

- Unmittelbare Unterstellung unter Dienststellenleitung
- Weisungsfreiheit
- Appellationsrecht
- Appellationsmöglichkeit für Beschäftigte
- Benachteiligungsverbot
- Freistellungserfordernis
- Einbindung in alle mit dem Schutz personenbezogener Daten in Zusammenhang stehende Angelegenheiten

Rechte und Pflichten

- Zugriffsbefugnisse
  - Einsichtsrecht in Dateien und Akten
  - kein generelles Zugriffsrecht
  - Zugriffsbefugnis im konkreten Einzelfall
- Einsicht in das Verzeichnis der Verarbeitungstätigkeiten (Art. 38 Abs. 1 DSGVO)
- Zeugnisverweigerungsrecht und Beschlagnahmeverbot
- Beratung durch die Aufsichtsbehörde
- Geheimhaltungs- und Verschwiegenheitspflicht (Art. 38 Abs. 5 DSGVO)

Unterstützungspflicht der Dienststelle

- Bereitstellung von
  - Hilfspersonal,
  - Räume,
  - der erforderlichen Zeit,
  - Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 der Datenschutzgrundverordnung,
  - Einrichtungen,
  - Geräte und
  - Mittel (z. B. Fachbücher, Kurse, Zeitschriften)
- Entbindung des Datenschutzbeauftragten von zeitraubenden sonstigen Aufgaben

Aufgaben (Art. 39 Abs. 1 DSGVO)

- Unterrichtung und Beratung
  - des Verantwortlichen
  - der Mitarbeiter/der Betroffenen
- Überwachung der Einhaltung der Datenschutzvorschriften
- Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter
- Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung
- Zusammenarbeit mit der Aufsichtsbehörde
- Anlaufstelle für die Aufsichtsbehörde

Sonstige möglichen Aufgaben

- Beteiligung und Überwachung der Datenschutz-Folgenabschätzung
- Führung von Verzeichnissen
- Beteiligung bei der Erstellung von Dienstanweisungen, und Dienstvereinbarungen bezüglich des Datenschutzes
- Mitwirkung bei der Einführung von IT-Systemen unter datenschutzrechtlicher Bewertung
- Prüfung der Zugriffsberechtigungen der Benutzer
- Beratung bei der Erstellung eines Sicherheitskonzepts
- Kontrolle der datenschutzgerechten Vernichtung von Datenträgern mit personenbezogenen Daten
- Überprüfung der Auftragsdatenverarbeitung hinsichtlich Vertragsgestaltung und Einhaltung der vorgegebenen Maßnahmen zum Datenschutz/Datensicherheit usw.

Weitere Informationsquellen

Orientierungshilfen und Informationen zur „Datenschutzreform 2018“ - abrufbar unter www.datenschutz-bayern.de

- Auftragsdatenverarbeitung bei der Aktenverwaltung in bay. öffentlichen und privaten Krankenhäusern
- Anforderungen an das Datenschutz-Management in bay. öffentlichen und privaten Krankenhäusern

Arbeitshilfen des Innenministeriums abrufbar unter https://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen/index.php

Vielen Dank für Ihre Aufmerksamkeit!

Noch Fragen?