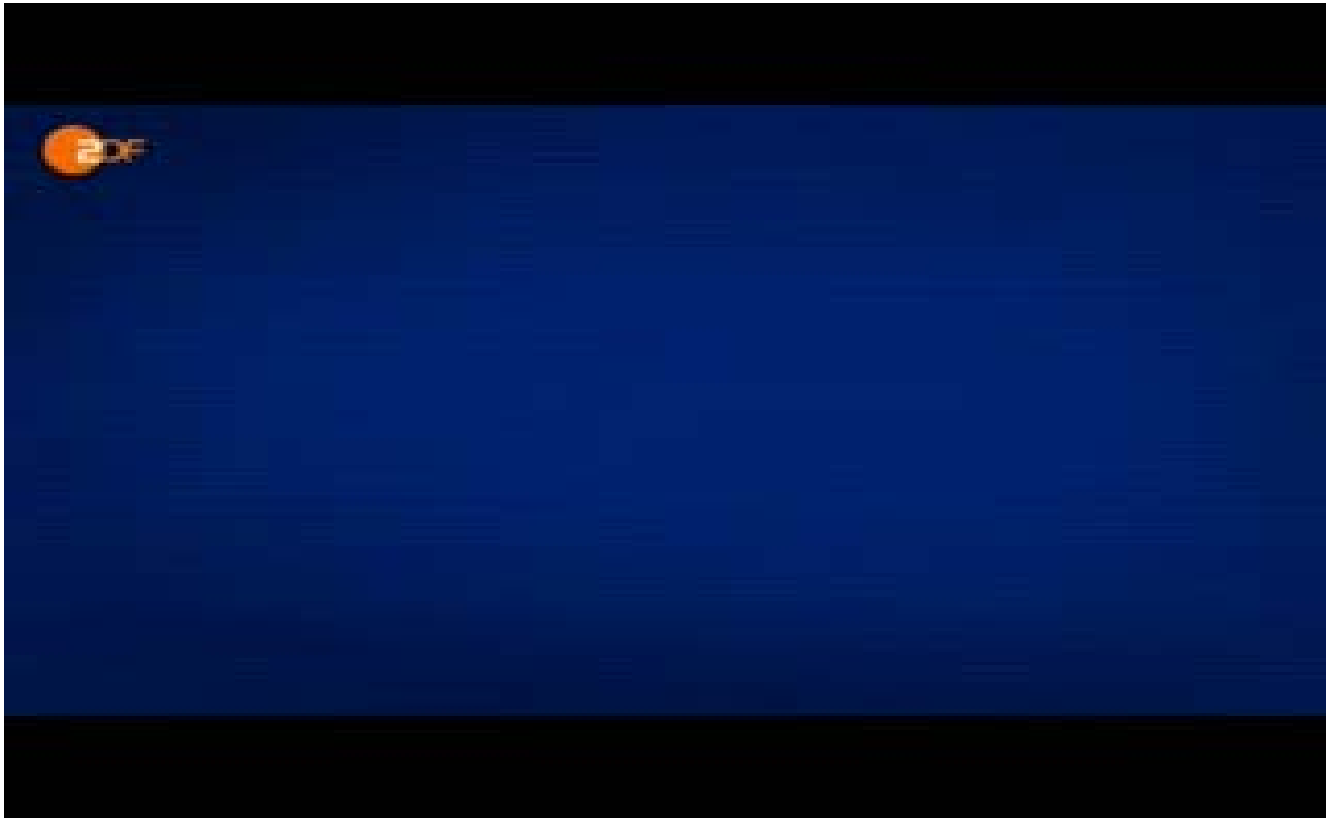
Schulung EU-DSGVO
Mitarbeiter/-innen der Hauptverwaltung

Personal

H. Kirch

28.02.2020

MDK MEDIZINISCHER DIENST DER KRANKENVERSICHERUNG NORDRHEIN


ZDF

EU-Datenschutzgrundverordnung

Meilenstein I

Das Bundesverfassungsrecht hat mit dem

Urteil vom 15.12.1983 (Volkszählungsurteil)

das Recht auf informationelle Selbstbestimmung geschaffen

EU-Datenschutzgrundverordnung

- Eigentum der Daten
- Keine belanglosen Daten
- Grundsatz der Zweckbestimmung
- Grundsatz der Erforderlichkeit
- Erlaubnisvorbehalt im Datenschutz
- Kein Eingriff ohne Rechtsgrundlage

EU-Datenschutzgrundverordnung

Datenschutz ist das
Grundrecht
zum Schutz der Privatsphäre

EU-Datenschutzgrundverordnung

Eckpunkte

- Inkrafttreten 25. Mai 2018 (Art. 99 EU-DSGVO)
- Meilenstein in der Weiterentwicklung des Datenschutzes
  - *Einheitliches Datenschutzrecht in der EU*
- Gestaltung als Verordnung
  - *Ablösung der EG-Datenschutzrichtlinie vom 24.10.1995*

EU-Datenschutzgrundverordnung

Eckpunkte

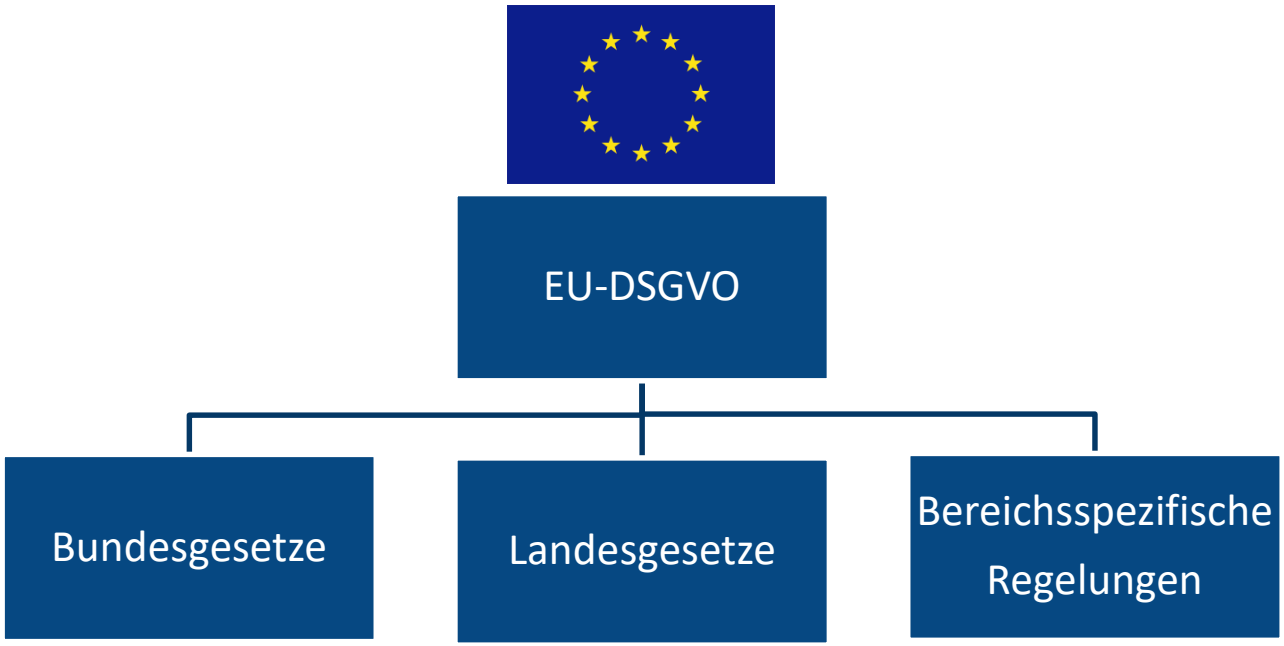
- Rechtscharakter
  - *Durchgriffswirkung*
- Öffnungsklausel
  - *ca. 50 bis 60 Öffnungsklauseln*

EU-Datenschutzgrundverordnung

Was ist geblieben?

Was ist neu?

EU-Datenschutzgrundverordnung



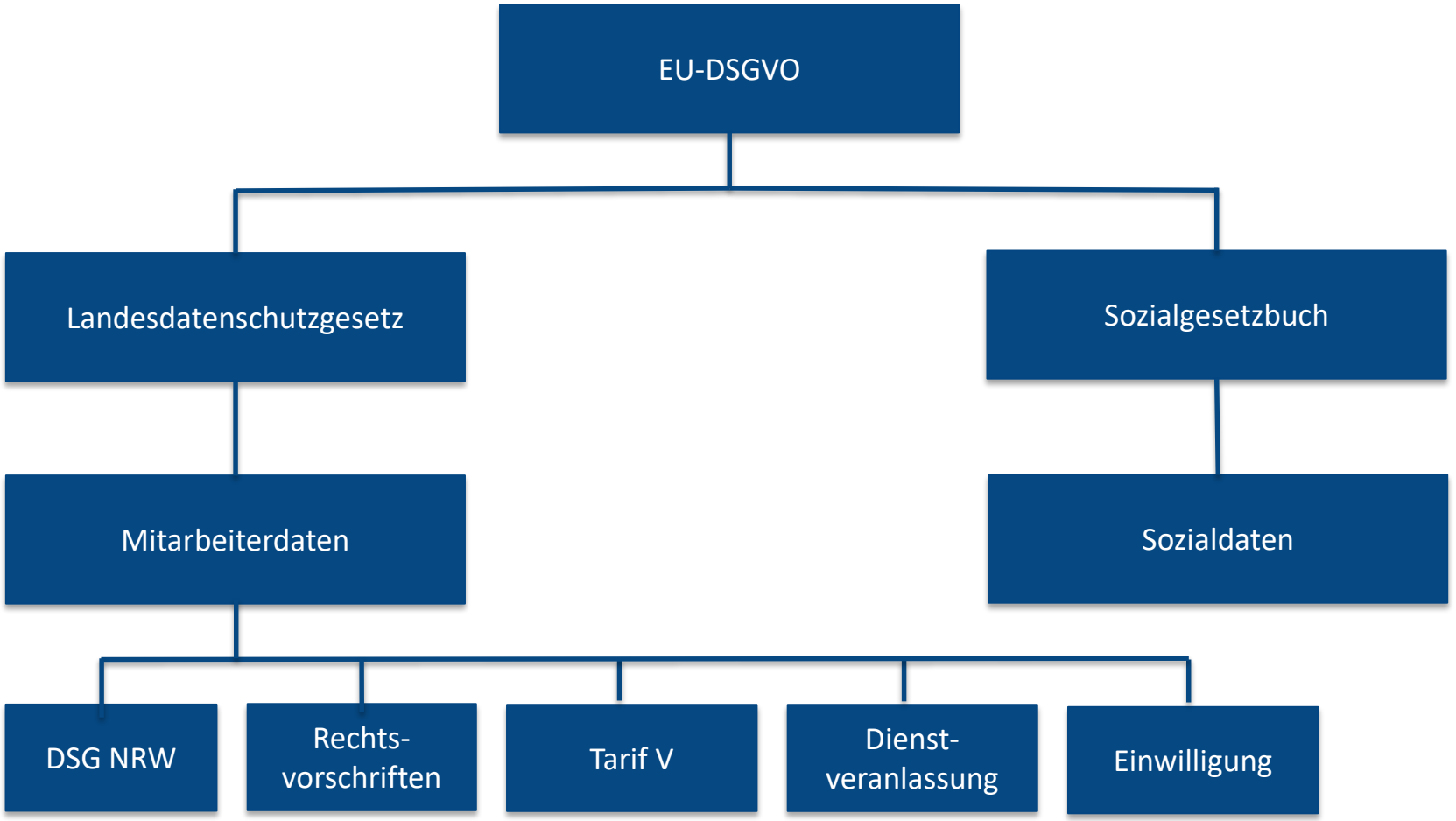
Bundesdaten-schutzgesetz § 26 BGSG

Landesdaten-schutzgesetz § 18 DSG NRW

Sozialgesetzbuch

EU-Datenschutzgrundverordnung

Systematik im Datenschutz



EU-Datenschutzgrundverordnung

Rechtsgrundlage

Worauf ist nach der

EU-DSGVO

der Blick zu richten?

EU-Datenschutzgrundverordnung

Rechtsgrundlage

Die Grundsätze

→ des Erlaubnisvorbehalt	Art. 6 u. 7 EU-DSGVO
→ der Einwilligung	Art. 6 Abs. 1 lit. a EU-DSGVO
→ der Erfüllung gesetzlicher Vorgaben	Art. 6 Abs. 2 lit. c u. e EU-DSGVO
→ der Erforderlichkeit	Art. 5 Abs. 1 lit. c EU-DSGVO
→ der Zweckbestimmung	Art. 5 Abs. 1 lit. b EU-DSGVO

behalten ihre Bedeutung.

EU-Datenschutzgrundverordnung

Anwendungsbereich

→ Personenbezogene Daten (Art. 4 Abs. 1 EU-DSGVO)

„Personenbezogene Daten sind alle Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und mit denen Rückschlüsse auf die Person möglich sind.“

– *Anwendung auf Daten Verstorbener*

- *Erwägungsgrund 27*

EU-Datenschutzgrundverordnung

Besondere Kategorien personenbezogener Daten

Die EU-DSGVO in Art. 9 versteht unter besonderen Kategorien von personenbezogener Daten:

„Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person …“

Die Verarbeitung dieser Daten ist untersagt. Ausnahmen davon sind im Art. 9 EU-DSGVO und in nationalen Regelungen näher geregelt.

EU-Datenschutzgrundverordnung

Besondere Kategorien personenbezogener Daten

Verarbeitung zulässig,

- → zur Erfüllung rechtlicher Verpflichtungen aus dem Arbeitsrecht
- → dem Recht der sozialen Sicherheit
- → des Sozialschutzes

EU-Datenschutzgrundverordnung

Besondere Kategorien personenbezogener Daten

- Kein Grund zu der Annahme besteht, dass die schutzwürdigen Interessen der betroffenen Person an dem Ausschuss der Verarbeitung besteht
- Anforderung an Einwilligung gilt auch für die Daten gem. Art. 9 EU-DSGVO
- Daten sind ausdrücklich in der Einwilligungserklärung auszuarbeiten

EU-Datenschutzgrundverordnung

Anwendungsbereich

→ Automatisierte/Dateigebundene Verfahren

– *Ganz oder teilweise automatisiertes Verfahren*

- *Speicherung in einem Dateisystem Art. 2 Abs. 1 EU-DSGVO manuelle Verfahren in strukturiertem Dateisystem*
- *Personalakte in Papierform*
- *Gehaltsakte in Papierform*
- *sonstige Akten in Papierform*

EU-Datenschutzgrundverordnung

Verarbeitung personenbezogener Daten

Verarbeitung Art. 4 Abs. 2 EU-DSGVO

→ Was bedeutet Verarbeitung im Sinne der EU-DSGVO

„Verarbeitung ist jede mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben…usw.“

EU-Datenschutzgrundverordnung

Anwendungsbereich

Normadressaten

- EU-DSGVO – Verantwortliche – Art. 4 Nr. 7 EU-DSGVO

  „Jede natürliche Person, Behörde, Einrichtung oder andere Stelle, die alleine oder gemeinsam über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden.“

- Mitarbeiter/-innen im Verantwortungsbereich der Personalverwaltung

EU-Datenschutzgrundverordnung

Wofür ist der Normadressat verantwortlich?

- Auswahl der Auftragsdatenverarbeitung
- Erfüllung der Rechte der Betroffenen
- Dokumentation-, Transparenz- und Rechenschaftspflichten
  - *Meldung von Datenpanne*
  - *Führung eines Verarbeitungsverzeichnisses*

EU-Datenschutzgrundverordnung

Wofür ist der Normadressat verantwortlich?

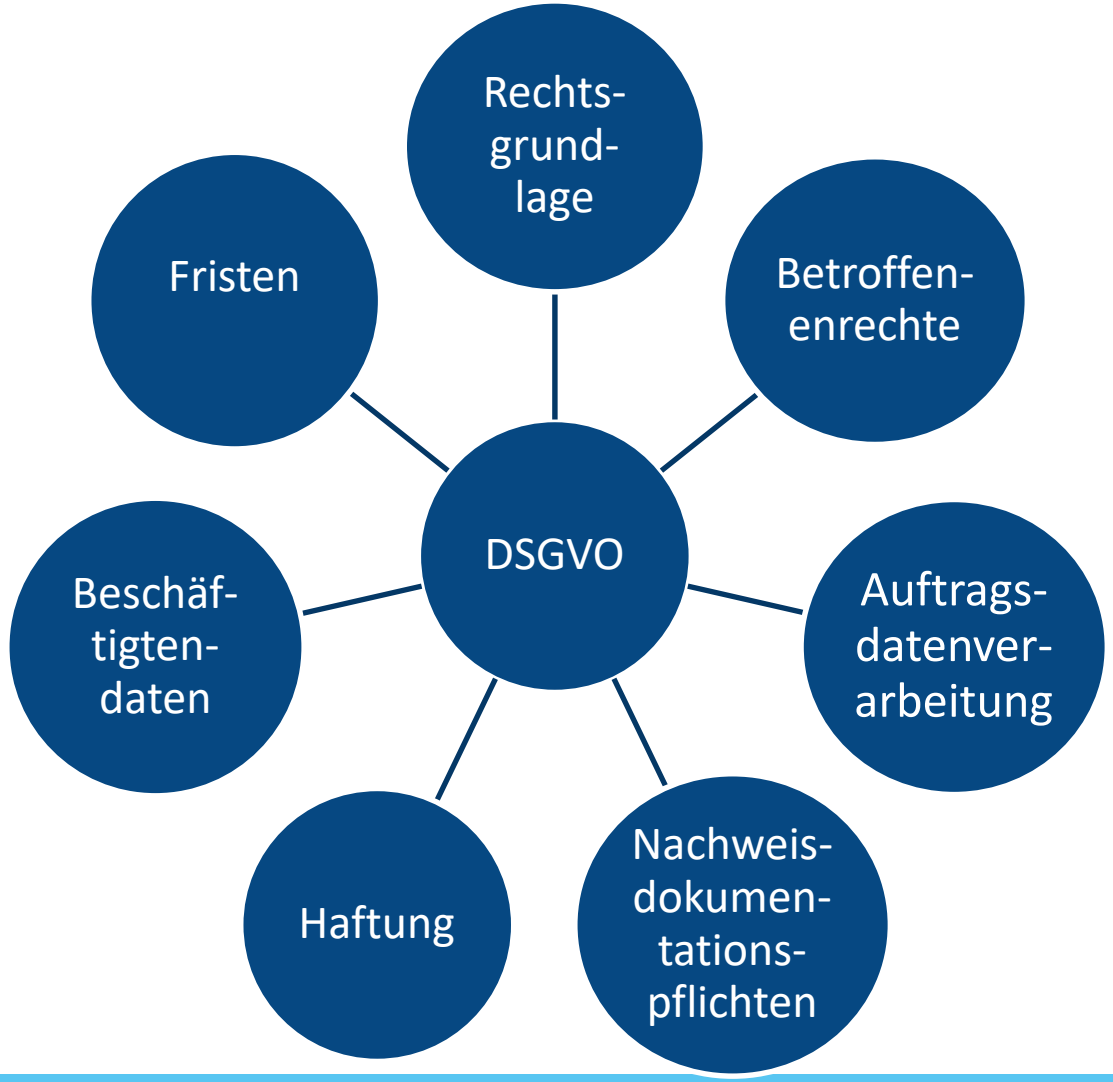
- → Zulässigkeit der Verarbeitung
- → Rechtmäßigkeit der Erhebung der Daten
- → Rechtmäßigkeit der Nutzung der Daten
- → Weitergabe der Daten an Dritte
- → Archivierung der Daten
- → Löschung der Daten

EU-Datenschutzgrundverordnung

Grundsatz der Vertraulichkeit

- Informationszugang nur für Befugte
  - *Zugriffskonzept*
  - *Verpflichtungserklärungen auf die Vertraulichkeit*
  - *Nachweis*

EU-Datenschutzgrundverordnung



EU-Datenschutzgrundverordnung

Rechtsgrundlagen für den Personalbereich

- Vertragserfüllung (Art. 6 Abs. lit. b DSGVO)
  - *Arbeitsvertrag*
- Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO)
  - *Rechtsnormen*
  - *Tarifvertrag*
  - *Dienstvereinbarungen*

EU-Datenschutzgrundverordnung

Rechtsgrundlagen für den Personalbereich

- Einwilligung (Art. 6 Abs. 1 lit. a DSGVO)
  - *Freiwillig*
  - *Schriftform*
  - *Widerrufsmöglichkeit*
  - *Getrennte Dokumentation*

EU-Datenschutzgrundverordnung

Rechtsgrundlage

→ Dienstvereinbarungen

- *SAP*
- *GLAZ*
- *ISmed3*
- *MDconnect*

EU-Datenschutzgrundverordnung

Rechtsgrundlage

- Datenverarbeitung im Beschäftigungskontext (§ 18 DSG NRW)
  - *Organisatorische, personelle und soziale Maßnahmen*
  - *Eingehung, Durchführung, Beendigung, Abweichung Beschäftigungsverhältnis*
  - *Personalplanung und Personaleinsatz*

EU-Datenschutzgrundverordnung

Rechtsgrundlage

Bewerbungen

- Softgarden – geregelter Ablauf
- Löschfristen
- Grundsätze:
  - *Löschung wenn hierzu kein Vertrag entsteht*
  - *Verlängerung – Einwilligungserklärung*
  - *AGG - Gleichbehandlungsgesetzt*

EU-Datenschutzgrundverordnung

Transparenzpflichten

- Informationspflichten
  - *Datenerhebung und Datenverarbeitung (Art. 13, 14 DSGVO)*
  - *Homepage*
  - *Information hieraus:*
    - *Vergabeverfahren*
    - *Verträge mit Externen*
    - *Kundenkontakt – Dienstleister/Versicherte*
    - *Call-Center*
    - *Pflege Informationsblätter*
    - *Mitarbeiterinformation*

EU-Datenschutzgrundverordnung

Transparenzpflichten

- Inhalte der Informationspflichten
  - *Kontaktdaten des Verantwortlichen*
  - *Zweck der Datenverarbeitung*
  - *Rechtsgrundlage der Datenverarbeitung*
  - *Empfänger der Daten*

EU-Datenschutzgrundverordnung

Transparenzpflichten

- *Dauer der Datenspeicherung/Löschfrist*
- *Rechte der Betroffenen*
- *Beschwerderecht*

EU-Datenschutzgrundverordnung

Rechte der Betroffenen

- Recht auf Auskunft
  - *Art. 15 EU-DSGVO*
- Recht auf Berichtigung
  - *Art. 16 EU-DSGVO*

EU-Datenschutzgrundverordnung

Rechte der Betroffenen

- Recht auf Löschung
  - *Art. 17 EU-DSGVO*
- Recht auf Einschränkung der Verarbeitung
  - *Art. 18 EU-DSGVO*

EU-Datenschutzgrundverordnung

Datenpanne

→ Rechtsgrundlage § 83 a SGB X oder § 59 DSG NRW

→ Datenpanne

Eine Datenpanne ist gemäß Art. 4 Nr. 12 DSGVO eine Verletzung des Schutzes personenbezogener Daten,

- *die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, führen.*

EU-Datenschutzgrundverordnung

Datenpanne

- *oder zur unbefugten Offenlegung beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet werden.*

Die Datenpanne im Sinne des Art. 4 Nr. 12 DSGVO, Art. 32 DSGVO ist in ihrem Anwendungsbereich umfassender Natur.

EU-Datenschutzgrundverordnung

Datenpanne

- Unverzügliche Anzeige an Vorgesetzten/Datenschutzbeauftragten
- Meldepflicht gegenüber Aufsichtsbehörde (72 Stunden Frist)
- Sozialdaten Meldepflicht gegenüber Rechtsaufsicht/Landesdatenschutzbehörde
- Leitfaden im Umgang mit einer Datenpanne
  - *Intranet*

EU-Datenschutzgrundverordnung

Datenschutzbeauftragter

- Bestellung eines Datenschutzbeauftragten
  - *Überwachungsfunktion*
  - *Beratungsfunktion*
  - *Ansprechstelle:*
    - *Verschwiegenheit*
  - *Schulung der Mitarbeiter/-innen*
  - *Weisungsunabhängigkeit bei Ausüben der Tätigkeit*

EU-Datenschutzgrundverordnung

Auftragsdatenverarbeitung

Definition

„Ein Auftragsverarbeiter ist nach der EU-DSGVO eine natürliche oder juristische Person, Behörde oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.“

EU-Datenschutzgrundverordnung

Pflichten in der Auftragsdatenverarbeitung

Auftraggeber

- → *Verantwortung bleibt beim Auftraggeber*
- → *Sorgfältige Auswahl des Dienstleisters*
- → *Schriftlicher Vertrag*
- → *Kontrolle und Überwachung*

EU-Datenschutzgrundverordnung

Pflichten in der Auftragsdatenverarbeitung

Auftraggeber

- → *Einräumung Zugangsrecht*
- → *Weisungsabhängigkeit*
- → *Prüfung der technischen und organisatorischen Vorkehrungen beim Auftragnehmer (Art. 28 Abs. 1 EU-DSGVO)*

EU-Datenschutzgrundverordnung

Pflichten in der Auftragsdatenverarbeitung

Auftragsnehmer

- → *Weisungsgebundenheit*
- → *Keine Unterauftragnehmer ohne Zustimmung*
- → *Meldepflicht bei Vorkommnissen*
- → *Einhaltung der datenschutzrechtlichen Verpflichtungen und Sicherung Art. 28 Abs. 3 c, 32 EU-DSGVO in Verbindung mit Art. 5 Abs. 1 und 2 EU-DSGVO*

EU-Datenschutzgrundverordnung

Pflichten in der Auftragsdatenverarbeitung

Auftragsnehmer

- → *Verpflichtung des Personals auf Datengeheimnis*
- → *Führen eines Verarbeitungsverzeichnisses*
- → *Regelung zu Rechten der Betroffenen*

EU-Datenschutzgrundverordnung

Pflichten in der Auftragsdatenverarbeitung

Meldepflichten

- → *Aufsichtsbehörde*
  - – *§ 80 SGB X (Sozialdaten)*
  - – *Beachtung im Verfahren*
- → *Prüfpflicht nach 2 Jahren, ob Voraussetzungen noch vorliegen.*
- → *Verwendung grundsätzlich MDK-Mustervertrag*
- → *Dokumentation*

EU-Datenschutzgrundverordnung

Verarbeitungsverzeichnis

Jede/Jeder Verantwortliche muss ein Verarbeitungsverzeichnis führen.

- → *Nachweis von Informations- und Dokumentationspflicht*
- → *Inhalt des Verarbeitungsverzeichnisses*
  - *Zweck der Verarbeitung*
  - *Empfänger der Datei*
  - *Kontaktdaten*
  - *Beschreibung der Daten*

EU-Datenschutzgrundverordnung

Verarbeitungsverzeichnis

- *Löschfristen*
- *Beschreibung der technischen und organisatorischen Maßnahmen*
- *Verwendung der internen Muster*
- *Durchführen einer Risikoanalyse über den Verarbeitungsprozess*
- *Durchführung einer Datenschutz-Folgenabschätzung (DSFA)*

EU-Datenschutzgrundverordnung

Speicherdauer und Aufbewahrungsfristen im Arbeitsverhalten

Grundsatz der Speicherbegrenzung

- → *Aufbewahrungsfristen*
  - *Keine Löschung, wenn die Daten zur Geltendmachung, Ausarbeitung und Verteidigung von Rechtsansprüchen erforderlich sind (Art. 17 Abs. 3 lit. e DSGVO)*
- → *Bewerberdaten*
  - *6 Monate nach Zeitpunkt der Absage*
- → *Dokumentation der Arbeitszeit*
  - *Mindestens 2 Jahre (ArbZG, JArbSchG, MikoC, MuSchG)*

EU-Datenschutzgrundverordnung

Speicherdauer und Aufbewahrungsfristen im Arbeitsverhalten

- *Unterlagen über Arbeitsfälle*
  - *3 Jahre als bindende Feststellung der Leistungspflicht (113 SGB VII)*
- *Ansprüche auf regelmäßige wiederkehrende Leistungen aus betrieblichen Altersversorgung*
- *Unterlagen mit steuerlicher Relevanz 6 bzw. 10 Jahre (§ 147 AO)*
- *Entgelt-Abrechnungsunterlagen 6 Jahre (§ 28 f. SGB IV, 147 AO)*
- *Lohnkarten 6 Jahre (§ 41 Abs. 1 S. 9. EStG)*

Vielen Dank für Ihre Aufmerksamkeit

Zusammenkommen ist ein Beginn

Zusammenbleiben ist ein Fortschritt

Zusammenarbeiten ist ein Erfolg