EU-Datenschutz-Grundverordnung und Beschäftigten-Datenschutz

Dr. Eva Angerler,
Abteilung Arbeit & Technik

Einführung
Betrieblicher Datenschutz

Rechtsgrundlagen Beschäftigtendatenschutz

- Datenschutz ist Grundrecht / „verfassungsgesetzlich gewährleistetes Recht“
- Recht auf Achtung des Privat- und Familienlebens (Art 8 EMRK); ständige Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR): auch am Arbeitsplatz gibt es eine Privatsphäre iSd Art 8 EMRK;
- Art 7 (Achtung des Privat- und Familienlebens) und Art 8 (Schutz personenbezogener Daten) der Charta der Grundrechte der Europäischen Union (GRC)
- betriebliche Ebene: §§ 96 und 96a ArbVG, § 10 AVRAG

Personenbezogene Daten – Legaldefinition (Art 4 EU-DSGVO)

- Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

- Als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

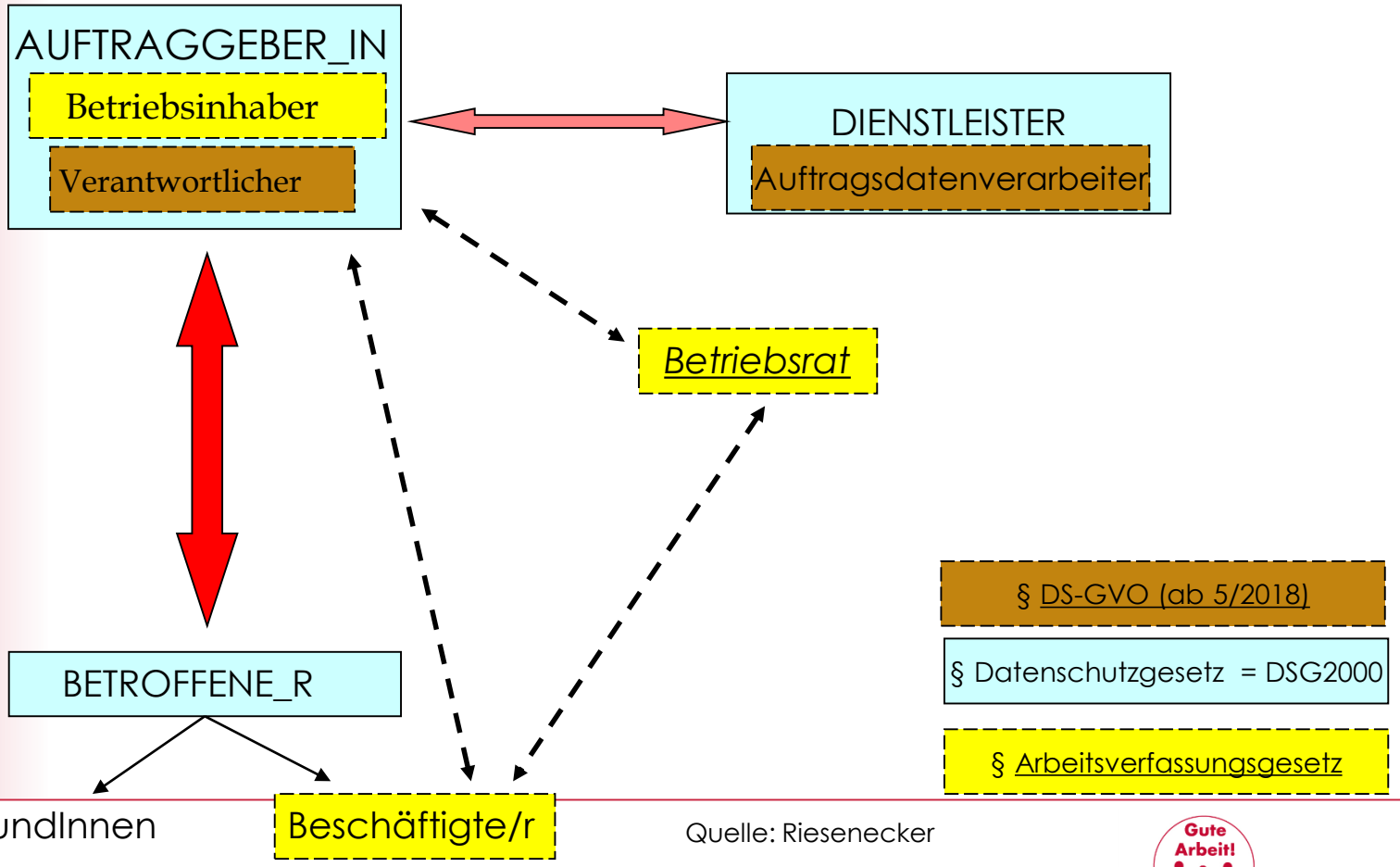
Daten im Betrieb

- Stammdaten (zB Name, Geschlecht, Adresse, Geburtsdatum)
- Qualifikationsdaten
- Gesundheitsdaten
- Bilddaten
- Bewegungsdaten
  - Arbeitszeitdaten
  - Gesprächsdaten
  - Daten über Leistung und Verhalten
- Protokolldaten (Logfiles)
- Sicherheitsspeicherungen

Systeme, die MitarbeiterInnen-Daten verarbeiten

- Kontrollsysteme
  - Zeiterfassungssysteme
  - Zutrittskontrollsysteme
  - Videoüberwachungssysteme
- Personalinformationssysteme
  - Stammdatenverwaltung, Module zu allen HR-Bereichen (Recruiting, Onboarding, Performancemanagement, usw.)
  - Standardisierung, Auswertungen zu Planungs- und Optimierungszwecken
- Kommunikationssysteme
  - Telefonsysteme, mobile Systeme (Smartphone, Tablet)
  - Internet und E-Mail
- Kollaborationssysteme (zB Yammer, Skype for Business)
- Standortdatensysteme (zB GPS, Mobilfunk-Tracking)
- …….

Rechtliche Ausgangssituation – Rollen



Quelle: Riesenecker

Die neue EU-Datenschutz-grundverordnung

EU-DS-Grundverordnung

- Seit 2012 verhandelt – 2016 beschlossen – 25.5. 2018 Inkrafttreten
- Rechtsform Verordnung: Direkt wirksam auf nationaler Ebene
- Datenschutz-Grundsätze annähernd gleich; tw weitergehend, tw unterschreitend
- Deutlich erhöhter Strafrahmen
  - 10 Mio. EUR oder 2 % des Jahresumsatzes
  - 20 Mio. EUR oder 4 % des Jahresumsatzes
- Deutlich gestärkte Rechtsdurchsetzung
  - Mehr Befugnisse für Aufsichtsbehörden
  - Bessere Koordination / Kooperation von Aufsichtsbehörden
  - Mehr Nachkontrolle statt Vorabprüfung

Grundsätze für die Verarbeitung personenbezogener Daten (Art 5 ff)

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung (festgelegte, eindeutige und legitime Zwecke)
- Datenminimierung (auf das für die Zwecke notwendige Maß beschränken)
- Richtigkeit (Daten aktuell halten, berichtigen, löschen)
- Speicherbegrenzung (Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange möglich macht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist)
- Integrität und Vertraulichkeit (technische und organisatorische Maßnahmen zum Schutz vor Verlust, Unbefugter und unrechtmäßiger Verarbeitung)

➢ **Rechenschaftspflicht:** Der Verantwortliche ist für die Einhaltung der DS-Grundsätze verantwortlich und muss deren Einhaltung nachweisen

➢ Betriebsvereinbarung soll Grundsätze und Betroffenenrechte abbilden

Rechte der betroffenen Person

- Klare und leicht verständliche Informationen bei Erhebung personenbezogener Daten (Art 13 und 14)
- Modalitäten für die effektive Ausübung der Rechte der Betroffenen bereitstellen (Informationen, Maßnahmen, Art 12)
- Recht auf Auskunft (Art 15), auf Berichtigung (Art 16), Recht auf Löschung von Daten/Recht auf Vergessenwerden (Art 17), Widerspruchsrecht (Art 21), Recht auf Datenübertragbarkeit (Art 20)
- Recht auf Beschwerde bei einer Aufsichtsbehörde, Recht auf gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde sowie Recht auf wirksamen, gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter (Art 77-79)
- Recht auf Ersatz des materiellen und/oder immateriellen Schadens wegen Verstoßes gegen die DSGVO (Art 82)
- Ausdrückliche Information bei automatisierter Entscheidungsfindung und Profiling
  - Aussagekräftige Infos über die involvierte Logik, die Tragweite und die angestrebten Auswirkungen einer derartigen Datenverarbeitung

Pflichten der Arbeitgeber

- mehr Selbstregulierung und neue Verpflichtungen
- Meldepflicht an ein Datenverarbeitungsregister fällt weg
- Verzeichnis von Verarbeitungstätigkeiten
- interne Maßnahmen zur Erfüllung der Datenschutz-Forderungen inkl Risikobewertung müssen dokumentiert werden
- Datensicherheit im Unternehmen nimmt hohen Stellenwert ein
- Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
- Datenschutz-Folgenabschätzung
- Meldung der Datenschutzverstöße
- Datenschutzbeauftragter (eingeschränkt)

Datenschutz durch Technik (Art 25)

- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
  - Technische und organisatorische Maßnahmen, zB Pseudonymisierung
  - Voreinstellung in Produkten, um Zweckbindung und Datensparsamkeit umzusetzen
  - Konzepte zum Löschen im Sinn des „Rechts auf Vergessen“
  - Zugriffseinstellungen
  - Genehmigtes Zertifizierungsverfahren als Nachweis für die Umsetzung der Anforderungen (Art 42)

Verzeichnis von Verarbeitungstätigkeiten (Art 30)

- Interne Dokumentation der Datenanwendungen verpflichtend
  - Name des Verantwortlichen, dessen Vertreter, Datenschutzbeauftragter
  - Zwecke der Verarbeitung
  - Kategorien betroffener Personen und personenbezogener Daten
  - Kategorien von Empfängern, incl. Empfänger in Drittländern
  - Übermittlungen von personenbezogenen Daten an Drittländer und Dokumentierung geeigneter Garantien
  - Löschfristen für die verschiedenen Datenkategorien
  - Beschreibung der technischen und organisatorischen Maßnahmen (Datensicherheitsmaßnahmen basierend auf Risikoanalyse, ev. Verhaltensregeln und Zertifizierung)
- Verzeichnis ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen

Sicherheit der Verarbeitung (Art 33)

- Verantwortliche und Auftragsverarbeiter haben geeignete technische und organisatorische Maßnahmen zu treffen, die den vorhandenen Risiken entsprechen, z.B.:
  - Pseudonymisierung und Verschlüsselung personenbezogener Daten
  - Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme sicherzustellen
  - Regelmäßige Evaluierung der Wirksamkeit
  - Genehmigte Verhaltensregeln oder Zertifizierung
  - Sicherstellung, dass die personenbezogenen Daten nur nach Anweisung des Verantwortlichen und Auftragsverarbeiters verarbeitet werden.

Meldung von DS-Verletzungen

- Verantwortlicher muss DS-Verletzungen binnen 72 Stunden ab Bekanntwerden an die Aufsichtsbehörde melden (Art 33)
- Meldung muss folgende Inhalte haben:
  - Art der Verletzung, betroffene Personen
  - Name und Kontaktdaten des DS-Beauftragten
  - Wahrscheinliche Folgen
  - Maßnahmen zur Behebung bzw. Abmilderung des Schadens
  - Dokumentation darüber zur Überprüfung durch die Aufsichtsbehörde
- Unverzügliche Benachrichtigung der betroffenen Person bei hohem Risiko (Art 34)

Datenschutzfolgenabschätzung (DSFA) - Art 35

- Datenverarbeitungen mit hohem Risiko für die Rechte und Freiheiten natürlicher Personen
  - Insb. bei automatisierten Einzelentscheidungen und Profiling (BIG DATA-Anwendungen), sowie bei Verwendung besonderer Datenkategorien
- Risikoeinschätzung
  - Beschreibung der Verarbeitungsvorgänge und der Zwecke
  - Bewertung der Verhältnismäßigkeit
  - Bewertung der Risiken für die Betroffenen
  - Abhilfemaßnahmen zum Schutz der Betroffenen
- Vorabkonsultationspflicht (Art 36)
  - Bei DV mit hohem Risiko und bei Fehlen von Maßnahmen zur Risikoeindämmung
  - Schriftliche Empfehlungen der Aufsichtsbehörde
- Listen von Datenanwendungen, für die DS-Folgenabschätzungen verpflichtend bzw. nicht verpflichtend sind, werden durch Datenschutzbehörden in EU erstellt
- Strafen bis 10 Mill € bei Nichteinhaltung

Verordnungen der DSB zu DSFA

- Whitelist (DSFA-AV): keine DSFA nötig bei (früheren Standardanwendungen), z.B.:
  - Personalverwaltung DSFA-A02
- Blacklist (DSFA-V): DSFA ist durchzuführen (durch BV in bestimmten Fällen ersetzbar), wenn z.B.:
  - Profile und Prognosen erstellt werden
  - Automatisierte Entscheidungsfindungen durchgeführt werden
  - Bestimmte Formen der Videoüberwachung
  - Künstliche Intelligenz angewendet wird, biometrische Daten verarbeitet werden
  - Algorithmische Entscheidungsfindungen unter Verwendung mehrerer Datenverarbeitungen
  - Umfangreiche Verarbeitung besonderer Datenkategorien
  - Erfassung von Standortdaten
  - Bestimmte Big Data Anwendungen

Datenschutzbeauftragte Art 37-39

- Verantwortliche und Auftragsverarbeiter benennen verpflichtend einen DSB in Öffentlichen Unternehmen (Behörden, öff. Stellen) und Unternehmen mit
  - Kerntätigkeit in Datenverarbeitung, die eine regelmäßige und systematische Überwachung von Betroffenen in großem Umfang erforderlich macht oder
  - Kerntätigkeit in der Verarbeitung besonderer (sensibler) Kategorien von Daten
  - Mitgliedsstaaten können Verpflichtung zum DS-Beauftragten erweitern
- Stellung und Aufgaben der DS-Beauftragten
  - Nicht weisungsgebunden
  - Dürfen nicht benachteiligt werden
  - Beratung des Verantwortlichen bzw. der Beschäftigten und Überwachung der Einhaltung der DSGVO
  - Bindeglied zu Aufsichtsbehörde
  - Sind keine verantwortlich Beauftragte

Verhaltensregeln und Zertifizierung – Art 40ff

- Verhaltensregeln auf Unternehmens- bzw. Branchenebene möglich
  - Freiwillig - selbst zu erarbeiten
  - Durch Aufsichtsbehörde zu genehmigen
  - Veröffentlichung
- Überwachung durch Aufsichtsbehörde - Zertifizierungen möglich – Aufsichtsbehörde akkreditiert Zertifizierungsorganisationen
- Verhaltensregeln und Zertifizierungen bringen Unternehmen international Vorteile
- Verbindliche interne Datenschutzvorschriften (Art 47)
  - Müssen ausdrücklich auch für Beschäftigte gelten

„One-stop-shop"-Prinzip

- Bei grenzüberschreitender Datenanwendung im Konzern innerhalb der EU
  - Aufsichtsbehörde der Hauptniederlassung in allfälligen Auseinandersetzungen federführend (Art 56)
  - Verantwortlicher für DS in EU muss benannt werden
  - Behörde im jeweils betroffenen Mitgliedstaat hat Überwachungsbefugnisse (Art 57-58)
  - Enge Zusammenarbeit zwischen den Behörden geboten (Art 60-62)
  - Kohärenzverfahren zur einheitlichen Rechtsanwendung (Art 63-67)

Grenzüberschreitende Datentransfers

- Genaue Festlegung, welche Daten zu welchem Zweck an wen übermittelt
- Blankoschecks sind nicht zulässig
- Durchsetzbare Rechte und wirksame Rechtsbehelfe für die Betroffenen sind Voraussetzung für Datentransfer ins Nicht-EU-Ausland (Art 44-49)
  - Grundlagen sind z.B.: Angemessenheitsbeschluss der EU, Standardvertragsklausen, verbindliche interne Datenschutzvorschriften;
- Betriebsvereinbarung wird in der Regel nötig sein

Strafen

- Geldbußen bis zu 20 Mill € oder 4% des weltweit erzielten Jahresumsatzes bei
  - Verstößen gegen DS-Grundsätze und Bedingungen für die Einwilligung gem. Art. 5,6,7 und 9
  - Verstößen gegen die Rechte der betroffenen Person (Art 12 bis 22)
  - Verstößen gegen die Bestimmungen betreffend Übermittlung personenbezogener Daten in ein Drittland (Art 44 bis 49)
- Geldbußen bis zu 10 Mill € oder 2% des weltweit erzielten Jahresumsatzes bei
  - Verstößen gegen die Pflichten der Verantwortlichen und der Auftragsverarbeiter (Art 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 42);
  - Die Pflichten der Zertifizierungsstelle (Art 42 und 43)
  - Verstößen gegen die Pflichten der Überwachungsstelle (Art 41 Abs 4)

AN-Datenschutz und DSGVO

- Öffnungsklausel in Art 88: Datenverarbeitung im Beschäftigungskontext: spezifischere Vorschriften durch Gesetz oder Kollektivvereinbarungen in den Mitgliedstaaten möglich
  - In Österreich ist ArbVG Vorschrift für Beschäftigtendatenschutz
- EWG 155: Betriebsvereinbarungen als Erlaubnistatbestand iSd DSGVO
- Bestehende und neue BVs müssen im Einklang mit der DSGVO stehen und die zentralen Grundsätze der DSGVO abbilden:
  - rechtmäßig, transparent, Zweckbindung, Datensparsamkeit, Datenaktualität, Löschung, Datensicherheit, Betroffenenrechte und Umgang mit besonderen Datenkategorien: genetische und biometrische Daten sowie strafrechtlich relevante Daten gelten auch als sensible Daten

Vertretung von betroffenen Personen (Art 80)

- Betroffene haben das Recht, eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht, … deren satzungsmäßige Ziele im öffentlichen Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, mit ihrer Vertretung zu beauftragen (Art 80 Abs 1)
- In Abs 2 wird den Mitgliedstaaten die Möglichkeit eingeräumt, solchen Einrichtungen, Organisationen oder Vereinigungen eine Art Verbandsklagerecht einzuräumen.

Die datenschutzrelevanten Bestimmungen des Arbeitsverfassungsgesetzes

Arbeitsrechtliche Grundlagen Rechte des Betriebsrats (1)

- **Kontrollrechte** (§ 89 ArbVG)
  - Überwachung der geltenden Rechtsvorschriften
- **Informationspflichten** (§ 91 Abs 2 ArbVG)
  - AG muss informieren, „welche Arten von personenbezogenen ArbeitnehmerInnendaten er automationsunterstützt aufzeichnet und welche Verarbeitungen und Übermittlungen er vorsieht"
  - AG muss „Überprüfung der Grundlagen für die Verarbeitung und Übermittlung ermöglichen"
- **Beratungsrechte** (§ 92 Abs 1 ArbVG)
  - „zumindest vierteljährlich" „in sozialer, personeller wirtschaftlicher und technischer Hinsicht"

Arbeitsrechtliche Grundlagen
Rechte des Betriebsrats (2)

- **Mitbestimmungsrechte** (§ 96 Abs 1 Z 3 ArbVG)
  - „Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der AN, die die Menschenwürde berühren"
  - ersatzweise Zustimmung des Gerichtes oder der Schlichtungsstelle ist *nicht* möglich

- **Mitbestimmungsrechte mit Zwangsschlichtung** (§ 96a Abs 1 Z 1 ArbVG)
  - bei „Systemen zur automationsunterstützten Ermittlung, Verarbeitung oder Übermittlung von personenbezogenen Daten des AN, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen"
  - Zustimmung des BR durch Entscheidung der Schlichtungsstelle ersetzbar

Arbeitsrechtliche Grundlagen – Rechte des Betriebsrats (3)

- **Allgemeine Ordnungsvorschriften (§ 97 Abs 1 Z 1)**
  - zB Arbeitszeitkontrollen durch Stechuhren, die nicht mit anderen Datensystemen verbunden sind, Verhaltenskodizes bzw. Compliance-Richtlinien
- **Maßnahmen zur zweckentsprechenden Benützung von Betriebseinrichtungen und Betriebsmitteln (§ 97 Abs 1 Z 6 ArbVG)**
  - Z.B.: Benützungsvorschriften für (Mobil)Telefone oder Internet bzw Email am Arbeitsplatz. Diesbezügliche Kontrollmaßnahmen, sofern sie die Menschenwürde berühren, sind aber zustimmungspflichtig nach § 96 ArbVG, uU kann auch § 96a ArbVG in Betracht kommen
- **AG kann allgemeine Weisungen erlassen – BR hat erzwingbares Mitbestimmungsrecht**

Betriebsvereinbarung über Kontrollsysteme

- Zielsetzung bzw. Verwendungszweck
- Welche personenbezogenen Daten werden ermittelt?
- Welche personenbezogenen Auswertungen werden gemacht?
- Welche personenbezogenen Daten werden übermittelt?
- Wann werden die Daten gelöscht?
- Rechte des BR (Information, Mitbestimmung, Kontrolle)
- Rechte der ArbeitnehmerInnen (Einsicht, Richtigstellung, Löschung)
- Vorgehen bei Einsichtnahme (stufenweise Kontrollverdichtung)
- Systembeschreibung als Bestandteil der BV

Es gibt vieles,

für das es sich lohnt,

organisiert zu sein.