



---

## **Expert Round Table: Datenschutz #disAbilityedition**

# I. Datenschutzrechtliche Grundlagen

## Einleitung

- **Datenschutzrecht in Österreich:**
  - **EU Datenschutz-Grundverordnung 2016/679**
    - Unmittelbar anwendbar seit 25. Mai 2018
  - **Datenschutzgesetz („DSG“)**
    - Geändert aus Anlass der DSGVO (Datenschutz-Anpassungsgesetz 2018)
  - **Datenschutzregeln auch in zahlreichen anderen Gesetzen:**
    - Arbeitsverfassungsgesetz: Schutz von Arbeitnehmerdaten (z.B. 96a ArbVG)

## Kategorien von Daten

- **Welche Daten sind erfasst?**
  - **Schutzniveau knüpft an Art der personenbezogene Daten an!**
  - **Personenbezogene Daten:** Angaben über Betroffene deren Identität bestimmt oder bestimmbar ist
  - Pseudonymisierte Daten
  - Fehlt der Personenbezug, gilt die DSGVO nicht!
    - Anonymisierung
- **Besonders geschützte Daten:**
  - **Besondere Kategorien von Daten iSd Art 9 DSGVO**  
(dazu später im Detail)
  - **Daten mit strafrechtlichem Bezug**

## Datenverarbeitung

- **Grundsatz:** Die Verarbeitung von Daten ist **verboten**
- **Aber:** Zulässigkeit der Datenverarbeitung unter Einhaltung der allgemeinen Grundsätze nach Art 5 DSGVO:
  - Rechtmäßigkeit
  - Verarbeitung nach Treu und Glauben
  - Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung
  - Integrität und Vertraulichkeit
  - Rechenschaftspflicht

## Rechtmäßigkeit der Verarbeitung

- Einwilligung
- Durchführung vorvertraglicher Maßnahmen
- Erfüllung eines Vertrags (auch: Arbeitsvertrag)
- Erfüllung einer rechtlichen Verpflichtung
- Lebenswichtige Interessen der betroffenen Person
- Wahrung der berechtigten Interessen
- Besonderheiten z.B. hinsichtlich
  - besonderer Kategorien personenbezogener Daten (Art 9 DSGVO)
  - Datenverarbeitung im Beschäftigungskontext (Öffnungsklausel Art 88 DSGVO)

## II. Besondere Kategorien von Daten

## Besondere Kategorien von Daten

- Personenbezogene Daten über
  - rassische und ethnische Herkunft
  - politische Meinungen
  - religiöse oder weltanschauliche Überzeugungen
  - Gewerkschaftszugehörigkeit
- Genetische Daten
- Biometrische Daten (z.B. Fingerabdruck)
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung

Graubereich: Bildaufnahmen



## Besondere Datenkategorie?



## Rechtsgrundlagen für besondere Datenkategorien

- Ausdrückliche Einwilligung
- Ausübung arbeitsrechtlicher und sozialrechtlicher Rechte bzw. Einhaltung diesbezüglicher Pflichten basierend auf nationalen Gesetzen, Kollektivverträgen oder Betriebsvereinbarungen
- Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- Gesundheitsvorsorge oder Arbeitsmedizin, Beurteilung der Arbeitsfähigkeit des Beschäftigten
- Vertrag mit einem Angehörigen eines Gesundheitsberufs

**Achtung:** kein berechtigtes Interesse als „Auffangbecken“

## III. Die vier Phasen des Arbeitsverhältnisses

### (1) Recruiting und Bewerbungsprozess

## (1) Recruiting und Bewerbungsprozess

- **Welche personenbezogenen Daten dürfen abgefragt werden?**

Grundsätzlich: Alle Informationen die für die Behandlung der Bewerbung und zur Beurteilung der Eignung eines Bewerbers für eine konkrete Stelle erforderlich sind (bedenke: Datenminimierung, Zweckbindung), das sind regelmäßig:

- Identifikationsdaten (Name, Geschlecht, Geburtsdatum, etc.)
- Kontaktdaten (Anschrift, Telefonnummer, E-Mail-Adresse, etc.)
- Staatsbürgerschaft
- Lebenslauf, beruflicher Werdegang
- Sonstige für die Eignung der ausgeschriebenen Stelle maßgebliche Daten (besondere Ausbildungen, Qualifikationen, etc.)

## (1) Recruiting und Bewerbungsprozess

- **Welche personenbezogenen Daten dürfen abgefragt werden?**

Sensible Informationen, wenn gewisse Voraussetzungen erfüllt sind:

- Informationen mit strafrechtlichem Bezug nur, wenn der Arbeitgeber aufgrund der konkreten Stelle ein berechtigtes Interesse hat (z.B. Wachdienst, Bankkassier, Geldtransport)
- Informationen zur Feststellung der Zugehörigkeit zum Kreis der begünstigten Menschen mit Behinderung, wenn die Stelle für einen begünstigten Menschen mit Behinderung iSd BEinstG vorgesehen ist
- Gesundheitsdaten, wenn es aufgrund der Rücksicht auf den Bewerber in Bezug auf die Stelle erforderlich ist (z.B. bei für Asthmatiker ungeeigneter Arbeitsumgebung)

## (1) Recruiting und Bewerbungsprozess

- **Welche personenbezogenen Daten dürfen abgefragt werden?**

Sensible Informationen, wenn gewisse Voraussetzungen erfüllt sind:

- Gesundheitsdaten, wenn eine ärztliche Untersuchung zur Feststellung der Eignung des Bewerbers gesetzlich vorgeschrieben ist oder sich aus der Art der Tätigkeit ergibt (z.B. im Gesundheitsbereich, Koch, Linienspilot)
- Frage nach ansteckenden Krankheiten zulässig?

## (1) Recruiting und Bewerbungsprozess

- **Welche personenbezogenen Daten dürfen nicht abgefragt werden?**
  - Vorliegen einer Schwangerschaft
  - Informationen über das Privatleben
  - Partei-, Religions- oder Gewerkschaftszugehörigkeit
  - Sexuelle Orientierung
  - Finanzielle Verhältnisse

## (1) Recruiting und Bewerbungsprozess

- **Ausgewählte Fragestellungen**

- Internet-Recherche zulässig (z.B. auf Social Media Plattformen)?
- Umgang mit nicht abgefragten Informationen, die vom Bewerber dennoch zur Verfügung gestellt werden?
- Einsatz von Head-Huntern und Vermittlungs-Agenturen? (Achtung: gegebenenfalls besondere Vereinbarung nach Artikel 26 DSGVO erforderlich)



## (1) Recruiting und Bewerbungsprozess

- **Wer darf Zugriff auf die Daten von Bewerbern haben?**

Nur diejenigen Mitarbeiter und Organe, die diese Informationen auch benötigen („Need-to-know-Prinzip“). Das sind regelmäßig:

- HR-Abteilung
- Entscheidungsträger in dem für den Bewerber vorgesehenem Bereich

Weitergabe von Bewerbungen innerhalb der Unternehmensgruppe?

## (1) Recruiting und Bewerbungsprozess

- **Wie lange dürfen Daten von Bewerbern aufbewahrt werden?**

Bewerbungen müssen nach spätestens **7 Monaten** ab dem Zeitpunkt, in dem feststeht, dass der Bewerber nicht genommen wird bzw. dem Bewerber eine Absage erteilt wird gelöscht werden (Hintergrund: §§ 12, 15 GlBG).

Möglichkeit zur längeren Aufbewahrung bzw. In-Evidenz-Haltung?

→ Einwilligung

## (1) Recruiting und Bewerbungsprozess

- **To-Do's aus datenschutzrechtlicher Sicht?**
  - Information der Bewerber bei Ausschreibung einer Stelle (Artikel 13 DSGVO)
  - Information von Bewerbern, die über Head-Hunter oder Agenturen vermittelt werden (Artikel 14 DSGVO)
  - ggf. Einholung einer Einwilligung (längere Aufbewahrung, Weitergabe in der Unternehmensgruppe)
  - Erforderlichenfalls Abschluss besonderer Vereinbarungen mit Head-Huntern und Vermittlungs-Agenturen

## III. Die vier Phasen des Arbeitsverhältnisses

### (2) Anstellung

## (2) Anstellung

- **Welche personenbezogenen Daten dürfen abgefragt werden?**

Grundsätzlich: Alle Informationen, die für die Begründung des Arbeitsverhältnisses erforderlich sind, das sind regelmäßig (zusätzlich zu den bereits aufgrund der Bewerbung vorhandenen Daten):

- Sozialversicherungsnummer und Sozialversicherungsträger
- Personenstand, Kinder und Familienangehörige im Zusammenhang mit Leistungen, die in Verbindung mit dem Arbeitsverhältnis erbracht werden
- Bankverbindung
- etc.

## (2) Anstellung

- **Wem dürfen die Daten übermittelt werden?**

Grundsätzlich: Es dürfen alle Übermittlungen erfolgen, die zur Begründung des Arbeitsverhältnisses und auf Grund der Gesetze erforderlich sind, beispielsweise:

- Anmeldung des Arbeitnehmers (idR vor Arbeitsantritt) bei der zuständigen Krankenkasse
- Meldung an die zuständige Lehrlingsstelle bei der Anstellung von Lehrlingen
- Anmeldung ausländischer Arbeitskräfte (die dem AuslBG unterliegen und keinen Aufenthaltstitel „Daueraufenthalt – EU“ haben) beim AMS

## (2) Anstellung

- **To-Do's aus datenschutzrechtlicher Sicht?**
  - Information der Arbeitnehmer (Artikel 13 DSGVO)
  - Verpflichtung auf das Datengeheimnis (§ 6 Abs 1 und 2 DSG)
  - Belehrung von Mitarbeitern über die für sie geltenden Übermittlungsanordnungen und über die Folgen der Verletzung des Datengeheimnisses (§ 6 Abs 3 DSG)
  - ggf. Einholung einer Einwilligung (z.B. Bildverwendung)

## III. Die vier Phasen des Arbeitsverhältnisses

### (3) Aufrechtes Arbeitsverhältnis



## (3) Aufrechtes Arbeitsverhältnis

- **Welche personenbezogenen Daten dürfen verarbeitet werden?**

Grundsätzlich: Alle Informationen die im Rahmen der Bewerbung und Anstellung des Bewerbers zulässig erhoben wurden (Personalakte) und alle Informationen, deren Verarbeitung im Zuge des Arbeitsverhältnisses erforderlich ist, wie beispielsweise:

- Ernährungsunverträglichkeiten im Falle von Flugbuchungen mit Verköstigung
- Informationen aus dem Fahrtenbuch im Falle der Verwendung von Dienstfahrzeugen
- Bildaufnahmen im Zuge von Videoüberwachung
- etc.

## (3) Aufrechtes Arbeitsverhältnis

- **Besonderheiten bei Verarbeitung von Gesundheitsdaten**

Informationen über den Gesundheitszustand von Arbeitnehmern können verarbeitet werden, wenn dies zur Erfüllung arbeits- und sozialrechtlicher Pflichten erforderlich ist, wie beispielsweise:

- Allgemeine Fürsorgepflicht (§§ 18 AngG, 6 ASchG):  
Berücksichtigung der Eignung von Arbeitnehmern in Bezug auf Sicherheit und Gesundheit bei der Übertragung von Aufgaben
- Rücksichtnahmepflicht bei begünstigten Menschen mit Behinderung (§ 6 BEinstG) und Schwangeren (§ 2a f MSchG) auf deren Gesundheitszustand bzw. Schwangerschaft

## (3) Aufrechtes Arbeitsverhältnis

- **Besonderheiten bei begünstigten Menschen mit Behinderung iSd BEinstG**
  - Führen eines Verzeichnisses: Name, Anschrift des Dienstnehmers, Beginn und Beendigung des Dienstverhältnisses, Versicherungsnummer, wesentlichen personenbezogenen Daten des Nachweises über die Zugehörigkeit zum Kreis der begünstigten Menschen mit Behinderung (§ 16 Abs 2 BEinstG)
  - Herausgabe des Verzeichnisses über Verlangen des AMS oder des Bundesamtes für Soziales und Behindertenwesen (§ 16 Abs 2 BEinstG)
  - Allgemeine Auskunftspflicht gegenüber amtlichen Organen, soweit dies im Interesse der begünstigten Menschen mit Behinderung erforderlich ist (§ 16 Abs 1 BEinstG)

## (3) Aufrechtes Arbeitsverhältnis

- **Wer darf Zugriff auf die Mitarbeiterdaten haben?**

Grundsätzlich nur diejenigen Mitarbeiter und Organe, die diese Informationen auch benötigen („Need-to-know-Prinzip“). Das sind regelmäßig:

- HR-Abteilung
- Buchhaltung
- Vorgesetzte
- Sonstige Abteilungen, welche die Daten benötigen

Weitergabe von Mitarbeiterdaten innerhalb der Unternehmensgruppe?

## (3) Aufrechtes Arbeitsverhältnis

- **Besonderheiten beim Zugriff auf Gesundheitsdaten**

Nur sehr eingeschränkter Personenkreis die Gesundheitsdaten nach dem „Need-to-know-Prinzip“, wie beispielsweise

- HR-Abteilung
- Vorgesetzte
- Für Sicherheit und Gesundheit der AN zuständige Personen (z.B. Sicherheitsvertrauensperson)

## (3) Aufrechtes Arbeitsverhältnis

- **Besonderheiten beim Zugriff auf Gesundheitsdaten**

§ 22a Abs 9 BEinstG:

*Der Betriebsinhaber ist verpflichtet, mit der Behindertenvertrauensperson (Stellvertreter) zu beraten und die zur Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen, insbesondere hat er die Behindertenvertrauensperson über substantielle, das Arbeitsverhältnis betreffende Angelegenheiten wie Beginn, Ende und Veränderung von Arbeitsverhältnissen behinderter Arbeitnehmer, über Arbeitsunfälle sowie über Krankmeldungen von mehr als sechs Wochen pro Kalenderjahr zu informieren.*

## (3) Aufrechtes Arbeitsverhältnis

- **Wem dürfen die Daten übermittelt werden?**

Grundsätzlich: Es dürfen alle Übermittlungen erfolgen, die zur Durchführung des Arbeitsverhältnisses und auf Grund der Gesetze erforderlich sind, beispielsweise:

- Anmeldung für Weiterbildungen bei externen Einrichtungen
- Buchung von Transportservices und Beherbergungen
- IT-Dienstleistern im Zuge von Service- und Wartungsdienstleistungen
- Meldung von Arbeitsunfällen an die AUVA
- Auskünfte gemäß § 16 BEinstG
- etc.

## (3) Aufrechtes Arbeitsverhältnis

- **Besonderheiten bei der Übermittlung von Gesundheitsdaten**

Grundsätzlich: Nur, wenn es auf Grund der Gesetze oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist, beispielsweise:

- Meldung von Arbeitsunfällen an die AUVA
- Auskünfte gemäß § 16 BEinstG
- Entlassung aufgrund vorgetäuschter Krankenstände

Weitergabe von Gesundheitsdaten innerhalb der Unternehmensgruppe?



## (3) Aufrechtes Arbeitsverhältnis

- **Wann und wie müssen Mitarbeiterdaten löschen?**

Grundsätzlich: Auch Löschung während aufrechten Arbeitsverhältnisses.

- Löschung in Entsprechung des internen Löschkonzepts (Näheres dazu unter Punkt III.(4))

## (3) Aufrechtes Arbeitsverhältnis

- **To-Do's aus datenschutzrechtlicher Sicht?**
  - Ggf. Anpassung der Information der Arbeitnehmer (Artikel 13 DSGVO)
  - Ggf. Information der Arbeitnehmer bei Zweckänderung (Artikel 14 Abs 4 DSGVO)
  - Ggf. Einholen von Einwilligungserklärungen
  - Ggf. Abschluss von Betriebsvereinbarungen
  - Laufend: Einhaltung des internen Löschkonzepts

## III. Die vier Phasen des Arbeitsverhältnisses

### (4) Beendigung des Arbeitsverhältnisses

## (4) Beendigung des Arbeitsverhältnisses

- **Grundsätzliches:**

- Zweckänderung von Durchführung und Abwicklung des aufrechten Arbeitsverhältnisses auf Beendigung des Arbeitsverhältnisses → Verarbeitung beschränkt sich auf diesen Zweck
- Grundsätzlich nur noch gesetzlich vorgesehene Übermittlungen (z.B. Meldung an Krankenkasse)
- Off-Boarding Arbeitnehmer
- Ab Beendigung: Hauptaugenmerk auf Aufbewahrung und Löschung gemäß internem Löschkonzept

## (4) Beendigung des Arbeitsverhältnisses

- **Wann müssen Mitarbeiterdaten gelöscht werden?**
  - Erstellung eines internen Löschkonzepts:
    - Festlegung von Löschfristen für die einzelnen Datenkategorien
    - Praktische und technische Umsetzung
  - Orientierung der Löschfristen an:
    - Verarbeitungszweck
    - gesetzliche Aufbewahrungspflichten
    - Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

## (4) Beendigung des Arbeitsverhältnisses

### • Löschfristen

- Löschung nach Wegfall des Verarbeitungszwecks (sofern eine Aufbewahrung nicht aus anderen Gründen geboten ist)

Beispiel: Nach dem Ausscheiden eines Arbeitnehmers sind seine Kontaktdaten nicht länger für die interne Telefonliste erforderlich und sind daher dort zu löschen.

- Löschung nach Ablauf der gesetzlichen Aufbewahrungspflicht (sofern eine Aufbewahrung nicht aus anderen Gründen geboten ist)

Beispiel: Daten betreffend Lohnsteuer- und Abgabepflicht sind 7 Jahre aufzubewahren (§ 132 Abs 1 BAO).

- Löschung nach Ablauf von Verjährungsfristen (sofern eine Aufbewahrung nicht aus anderen Gründen geboten ist)

Beispiel: Schadenersatzansprüche des Arbeitgebers gegenüber dem Arbeitnehmer verjähren in der Regel in 3 Jahren (§ 1489 ABGB).

## (4) Beendigung des Arbeitsverhältnisses

- **Wie müssen Mitarbeiterdaten gelöscht werden?**
  - Löschen ≠ Löschen
    - Sperren / Einschränken
    - unbenutzbar / unlesbar machen
    - Anonymisieren
    - Physisches Löschen
  - Löschen in allen Systemen und Löschen von Kopien
  - Implementierung entsprechender Löschroutinen
  - Löschen aus automatischem Backup?

## (4) Beendigung des Arbeitsverhältnisses

- **To-Do's aus datenschutzrechtlicher Sicht?**
  - Off-Boarding (Rückgabe von Geräten, Mitnahme privater Gegenstände, Löschung privater E-Mails)
  - Ggf. Bestätigung über Off-Boarding und Erinnerung an Datengeheimnis
  - Einhaltung des internen Löschkonzepts



# CHSH

Cerha Hempel Spiegelfeld Hlawati  
Rechtsanwälte GmbH

---

Vielen Dank für Ihre Aufmerksamkeit!