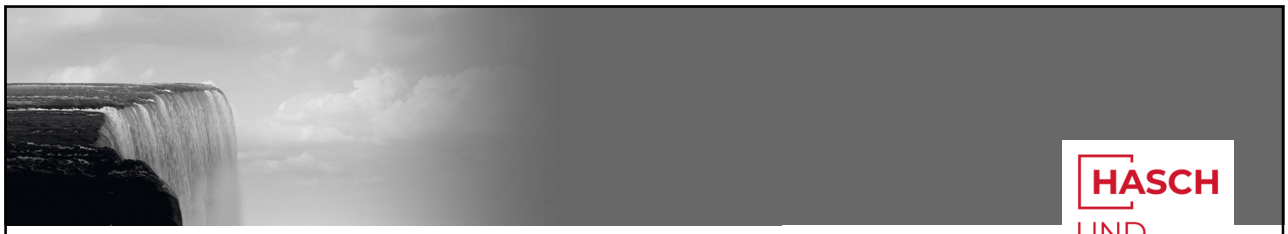
COMPLIANCE SEMINAR
BASISMODUL DATENSCHUTZRECHT

RECHTSANWALT MAG. JOHANNES WOLFGRUBER, MBA

Linz, am 17.01.2024

INHALTSVERZEICHNIS



INHALTSVERZEICHNIS

1.
EINFÜHRUNG UND RECHTSGRUNDLAGEN

EINFÜHRUNG UND RECHTSGRUNDLAGEN (1)

- Daten: wirtschaftlich sehr bedeutend
- Datenverarbeitung: gesetzlich reglementiert
  - EU: - Datenschutzgrundverordnung (DSGVO): unionsweit einheitlich, unmittelbar anwendbar
  - Österreich: - Datenschutzgesetz (DSG) Grundrecht auf Datenschutz (§ 1 DSG)
    - Telekommunikationsgesetz (TKG)

EINFÜHRUNG UND RECHTSGRUNDLAGEN (2)

- Bei Verstößen: Strafen bis zu EUR 20 Mio. oder 4 % des Jahresumsatzes

  Datenverarbeitung grundsätzlich verboten!

  Außer es liegt eine gesetzliche Ausnahme vor.

GRUNDSÄTZE DER DATENVERARBEITUNG

- rechtmäßig, nach Treu und Glauben und transparent
- Zweckbindung:
  - nur für festgelegte eindeutige Zwecke
  - nicht in mit diesen Zwecken unvereinbarer Weise weiterverarbeiten
- Datenminimierung:
  - nur so viele Daten verarbeiten, wie zur Zweckerreichung nötig
- Richtigkeit:
  - sachlich richtig
  - aktuell

GRUNDSÄTZE DER DATENVERARBEITUNG (1)

- Speicherbegrenzung:
  - nur so lange speichern, wie für den Zweck erforderlich (Löschung!)
- Integrität/Vertraulichkeit:
  - Datensicherheit
  - organisatorische und technische Schutzmaßnahmen
- Rechenschaftspflicht:
  - Der Verantwortliche muss die Einhaltung der Grundsätze nachweisen können!

GRUNDSÄTZE DER DATENVERARBEITUNG (2)

- Rechtmäßig: - Rechtsgrundlage erforderlich
- Nach Treu und Glauben: - fair, Interessensabwägung
- Transparent: - in einer für den Betroffenen nachvollziehbaren Weise

ANWENDUNGSBEREICHE DER DSGVO

- Sachlich
  - Jede automatisierte Verarbeitung von **personenbezogenen Daten**, die in einem System gespeichert werden sollen (auch analog).
- Räumlich
  - Datenverarbeitung in der EU (inkl. "Datenexport" in Drittländer)
  - Marktauftreten in der EU (betroffene Person in der EU)

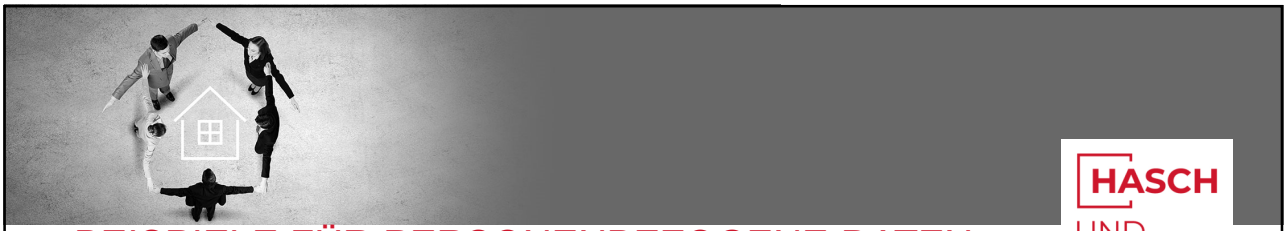
2.
PERSONENBEZOGENE DATEN / DATENARTEN

PERSONENBEZOGENE DATEN

- DSGVO gilt für <u>personenbezogene Daten:</u>
  - alle Informationen, die sich auf natürliche Personen beziehen
  - auch solche, die eine Person identifizierbar machen
  - auch pseudonymisierte Daten
  - unabhängig vom Format (schriftlich, Audio, Video, digital, analog,…)
  - unabhängig vom Betroffenenkreis (Kunden, Lieferanten, Mitarbeiter,…)

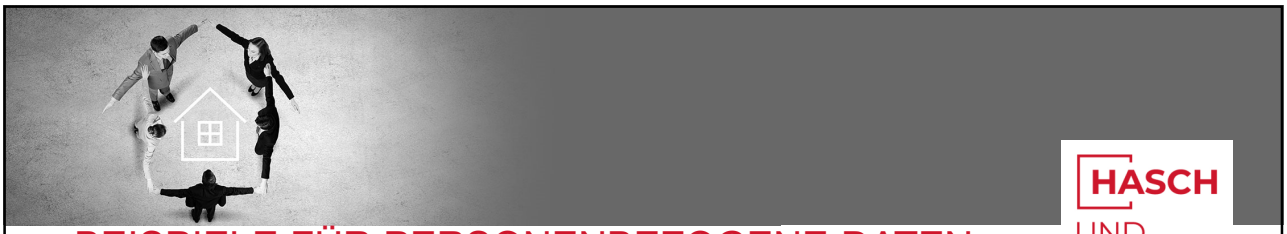
PERSONENBEZOGENE DATEN

- Nicht umfasst:
  - rein private/familiäre Zwecke (ohne Unternehmensbezug)
  - anonymisierte Daten (wenn nicht mehr auf einzelne Betroffene rückführbar)



BEISPIELE FÜR PERSONENBEZOGENE DATEN (1)

- Name (Vorname, Nachname, auch Pseudonyme, Benutzernamen und Onlinekennungen)
- Geburtsdatum, Alter
- Adress- und Standortdaten
- Sozialversicherungsnummer, Steuernummer, Ausweisnummer
- IP-Adresse



BEISPIELE FÜR PERSONENBEZOGENE DATEN (2)

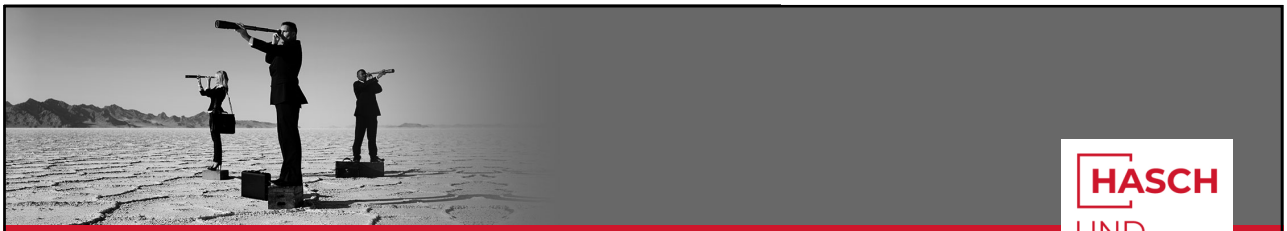
- Informationen über persönliche Neigungen, Interessen, Hobby, etc.
- Informationen über familiäre Verhältnisse / Familienstand
- Telefonnummer
- E-Mail-Adresse
- Informationen über Ausbildung, berufliche Tätigkeit, Einkommen, Gehalt
- etc.

BESONDERE DATENKATEGORIEN ("SENSIBLE DATEN") (1)

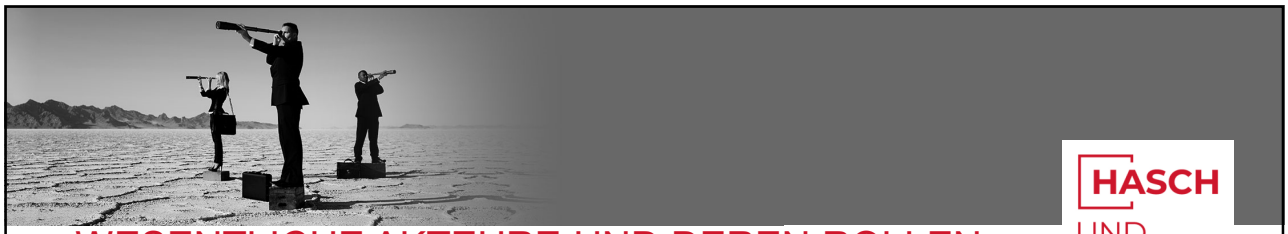
- strengere Voraussetzungen für die Datenverarbeitung bei besonderen Datenkategorien:
  - rassische und ethnische Herkunft
  - politische Meinungen
  - religiöse oder weltanschauliche Überzeugungen

BESONDERE DATENKATEGORIEN ("SENSIBLE DATEN") (2)

- Gewerkschaftszugehörigkeit
- genetische und biometrische Daten
- Gesundheitsdaten
- Daten zum Sexualleben / zur sexuellen Orientierung
- noch strenger: Daten über strafrechtliche Verurteilungen und Straftaten



3. AKTEURE UND ROLLENVERTEILUNG



WESENTLICHE AKTEURE UND DEREN ROLLEN (1)

- Verantwortlicher:
  - derjenige, durch den oder in dessen Auftrag die Daten erhoben und verarbeitet werden
  - entscheidet darüber, dass Daten verarbeitet werden und über Zwecke und Mittel der Datenverarbeitung
  - auch mehrere Verantwortliche sind möglich ("gemeinsame Verantwortliche"
    ⇨ Vertrag ist erforderlich zur Regelung der DSGVO-Verpflichtungen)

WESENTLICHE AKTEURE UND DEREN ROLLEN (2)

- Auftragsverarbeiter:
  - verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen
  - entscheidet **nicht** über Zwecke und Mittel der Datenverarbeitung
- Betroffene Person:
  - natürliche Person, auf welche sich die Informationen/Daten beziehen
- Empfänger:
  - Person, der die personenbezogenen Daten offen gelegt werden

4.
ZULÄSSIGE DATENVERARBEITUNG

RECHTMÄßIGKEIT DER DATENVERARBEITUNG (1)

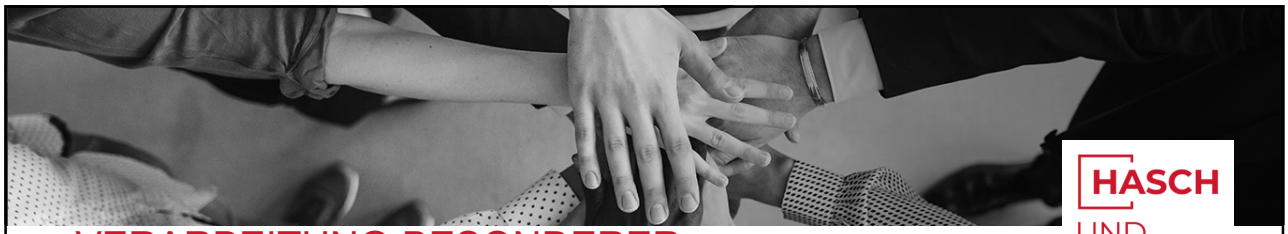
- **Irrglaube:** man benötigt **stets** eine Einwilligung!
- verschiedene Rechtsgrundlagen für zulässige Datenverarbeitung möglich (Einwilligung nicht zwingend)

RECHTMÄßIGKEIT DER DATENVERARBEITUNG (2)

- Datenverarbeitung ist erlaubt, wenn mind. eine der folgenden **Voraussetzungen** erfüllt ist (Art 6 DSGVO):
  - **Einwilligung** des Betroffenen für den bestimmten Zweck
  - Erforderlichkeit zur **Erfüllung eines Vertrages** (mit dem Betroffenen) oder für vorvertragliche Maßnahmen
  - Erforderlichkeit zur Erfüllung einer **rechtlichen Verpflichtung**

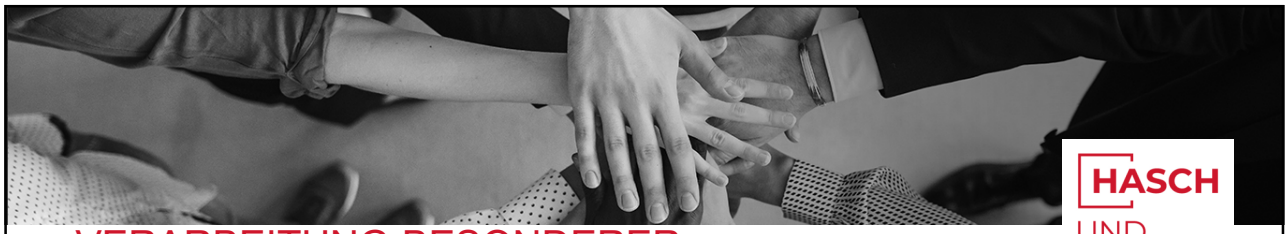
RECHTMÄßIGKEIT DER DATENVERARBEITUNG (3)

- Erforderlichkeit zum Schutz **lebenswichtiger Interessen**
- Erforderlichkeit zur Wahrnehmung einer Aufgabe im **öffentlichen Interesse**
- Erforderlichkeit zur Wahrung **berechtigter Interessen** des Verantwortlichen oder eines Dritten, sofern nicht die Interessen des Betroffenen überwiegen
- ⇨ wichtig: Interessensabwägung!



VERARBEITUNG BESONDERER DATENKATEGORIEN (1)

- nur erlaubt (Art 9 DSGVO):
  - bei **ausdrücklicher Einwilligung** des Betroffenen für den bestimmten Zweck
  - bei Erforderlichkeit iZm Rechten und Pflichten aus dem **Arbeits- und Sozialrecht**
  - bei Erforderlichkeit zum Schutz **lebenswichtiger Interessen**, wenn Einwilligung nicht möglich
  - durch eine **Non-Profit Organisation** iZm mit ihren Mitgliedern



VERARBEITUNG BESONDERER DATENKATEGORIEN (2)

- wenn Betroffener die Daten **selbst öffentlich gemacht** hat
- bei Erforderlichkeit zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen**
- bei Erforderlichkeit für Zwecke im **Gesundheitsbereich**
- bei (erheblichem) **öffentlichen Interesse**

WIRKSAME EINWILLIGUNG – VORAUSSETZUNGEN (1)

- Rechtzeitigkeit: Einwilligung **vor** Erhebung und Verwendung der Daten einholen
- **verständliche** und leicht zugängliche Form, **klare und einfache Sprache**
- muss für Betroffenen **klar erkennbar** sein und sich vom restlichen Text abheben
- Einwilligung hat **in informierter Art und Weise** zu erfolgen (dh. der Betroffene muss über die Datenarten, den konkreten Zweck, und durch wen die Daten verarbeitet werden bzw. an wen sie übermittelt werden, informiert sein)

WIRKSAME EINWILLIGUNG – VORAUSSETZUNGEN (2)

- Freiwilligkeit ohne Zwang, keine Kopplung, Nichterteilung der Einwilligung darf für Betroffenen keinen Nachteil bringen
- **aktive** Handlung/Erklärung des Betroffenen (keine vorangekreuzten Kästchen, Schweigen gilt nicht als Zustimmung)
- **Nachweispflicht** für den Verantwortlichen (Schriftlichkeit nicht zwingend, aber empfohlen!)
- Widerrufbarkeit: Jederzeitiger Widerruf muss möglich sein (Widerrufsbelehrung erforderlich!)

EINWILLIGUNG MINDERJÄHRIGER

- ab vollendetem **14. Lebensjahr**:
  wirksame Einwilligung möglich ("**digitale Mündigkeit**")
  (gilt für Österreich gemäß § 4 Abs 4 DSG; in anderen Mitgliedsstaaten zT andere Altersgrenzen)
- Einwilligungen von unter 14-jährigen sind unwirksam
  (Einwilligung des Erziehungsberechtigten erforderlich)
- geeignete Maßnahmen setzen, um Alter festzustellen

FREIWILLIGKEIT DER EINWILLIGUNG

Freiwilligkeit liegt nur vor, wenn:

- Einwilligung ohne Zwang oder unangemessenen Druck erteilt wird
- keine beträchtlichen Nachteile bei Nichterteilung der Einwilligung drohen
- kein starkes Abhängigkeitsverhältnis besteht (zB sind Einwilligungen im Rahmen eines Arbeitsverhältnisses oft unwirksam)

FREIWILLIGKEIT DER EINWILLIGUNG

- keine Koppelung mit der Erbringung vertraglicher Leistungen erfolgt: Wird die Erfüllung eines Vertrages oder die Erbringung einer Dienstleistung daran geknüpft, dass eine Einwilligung zur Verarbeitung von Daten erteilt wird, die zur Vertragserfüllung gar nicht erforderlich sind, ist dies unzulässig ("Koppelungsverbot")

KOPPELUNGSVERBOT: BEISPIEL (1)

Beispiel: Die Bestellung in einem Webshop erfordert die Angabe der Liefer- und Rechnungsadresse. Für die Zusendung einer Bestellbestätigung ist eine E-Mail-Adresse notwendig. Der Webshop verknüpft die Zusendung der Bestellbestätigung mit der Einwilligung zum Erhalt eines Newsletters zu Werbezwecken.

⇨ **unzulässige Koppelung**, da Werbezusendungen nicht für die Erfüllung des Vertrages erforderlich sind

KOPPELUNGSVERBOT: BEISPIEL (2)

Kann der Kunde die Zusendung nicht ablehnen, ohne auf den Kauf zu verzichten, ist eine Einwilligung nicht freiwillig erteilt worden. Die Zusendung von Werbung erfolgt somit ohne gültige Rechtsgrundlage. Selbst die nachträgliche Abmeldemöglichkeit von einem Newsletter macht die Datenverarbeitung nicht rechtmäßig.

RECHTSGRUNDLAGE: VERTRAGSERFÜLLUNG

- "Vertragserfüllung" ist einer der häufigsten Rechtfertigungsfälle
- wenn die Datenverarbeitung für die Erfüllung eines Vertrages mit dem Betroffenen oder zur Durchführung vorvertraglicher Maßnahmen auf Anfrage des Betroffenen erfolgt
- wenn Datenverarbeitung zur Vertragserfüllung notwendig: keine Einwilligung erforderlich

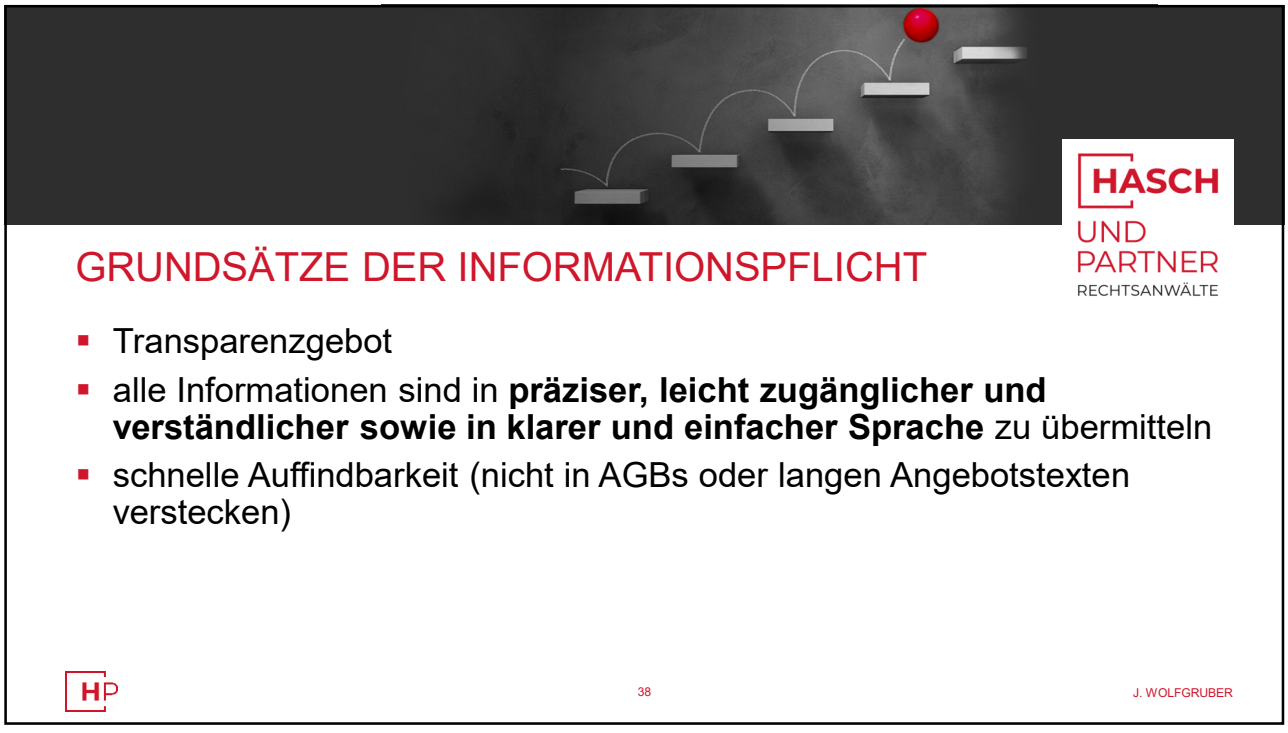
RECHTSGRUNDLAGE: BERECHTIGTE INTERESSEN

- Interessenabwägung im Einzelfall erforderlich
  - Interessen des Betroffenen auf Schutz der Daten dürfen nicht überwiegen
- Beispiele für berechtigte Interessen:
  - Verhinderung von Betrug, Leistungsmissbrauch, Geldwäsche
  - "Konzerndatenverwaltung"

RECHTSGRUNDLAGE: BERECHTIGTE INTERESSEN

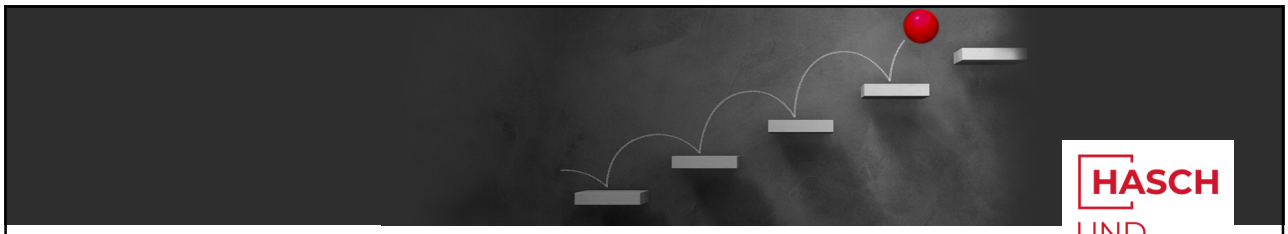
- Überwachung von Arbeitnehmern aus Sicherheits-/Verwaltungs-gründen
- Wirtschaftliche Interessen (zB Kennzeichenerfassung in Parkgaragen)
- statistische Zwecke
- Forschungszwecke (auch Marktforschung)

5.
INFORMATIONSPFLICHTEN



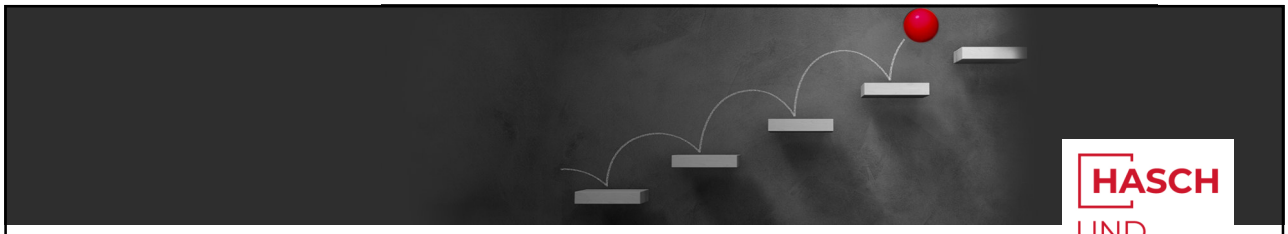
GRUNDSÄTZE DER INFORMATIONSPFLICHT

- Transparenzgebot
- alle Informationen sind in **präziser, leicht zugänglicher und verständlicher sowie in klarer und einfacher Sprache** zu übermitteln
- schnelle Auffindbarkeit (nicht in AGBs oder langen Angebotstexten verstecken)



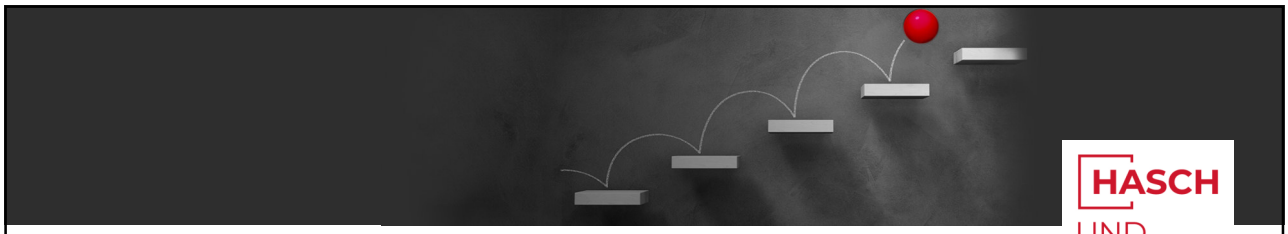
INFORMATIONSPFLICHTEN (AKTIV)

- Umfassende Information, vorzugsweise durch schriftliche **Datenschutzerklärung**, zB via:
  - Website
  - Verlinkung zur Datenschutzerklärung auf der Website
  - QR-Code
  - Pop-Up Benachrichtigung
  - Beiblatt zum Vertrag
  - Übermittlung per E-Mail/Post
  - Persönliche Aushändigung in Papierform
  - Aufsteller / Schild



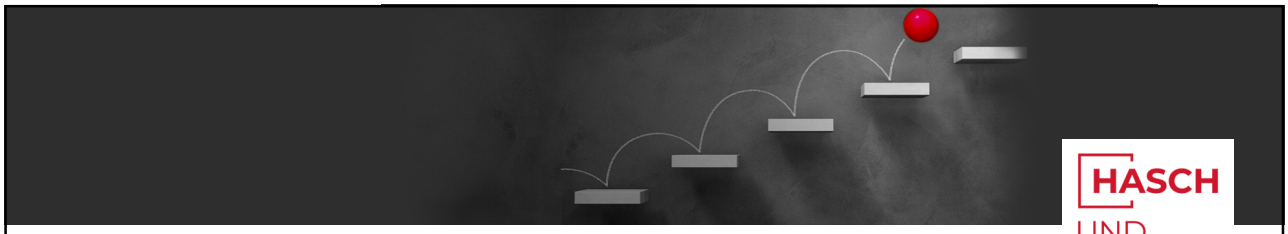
UMFANG DER INFORMATIONSPFLICHT (1)

- Verantwortlicher (Name und Kontaktdaten)
- Datenschutzbeauftragter (Name und Kontaktdaten)
- Zwecke, für welche die Daten verarbeitet werden, und die Rechtsgrundlage für die Verarbeitung
- ggf. berechtigte Interessen
- ggf. Empfänger bzw. –kategorien
- ggf. beabsichtigte Drittstaatentransfers inkl. Verweise auf Angemessenheitsbeschlüsse bzw. Garantien



UMFANG DER INFORMATIONSPFLICHT (2)

- Speicherdauer
- Betroffenenrechte
- ggf. Widerrufsmöglichkeit (sofern Einwilligung)
- Beschwerderecht bei Aufsichtsbehörde
- Verpflichtung zur Bereitstellung
- Profiling



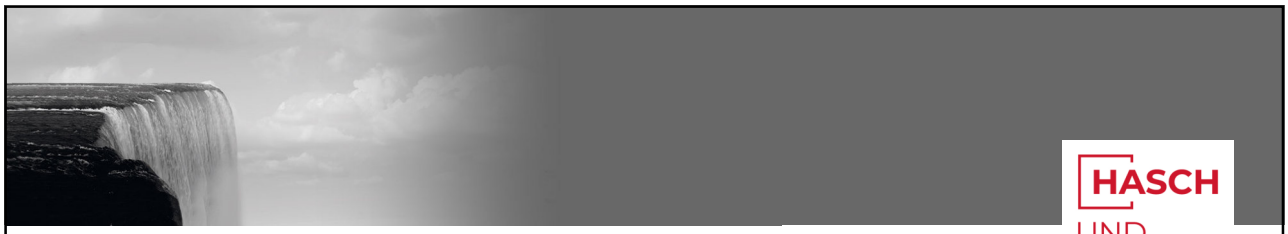
ZEITPUNKT DER INFORMATION

- wenn Datenerhebung beim Betroffenen:
  ⇨ **zum Zeitpunkt der Datenerhebung** bzw. vor der Weiterverarbeitung
- wenn Datenerhebung nicht beim Betroffenen:
  ⇨ grds. innerhalb angemessener Frist nach Erlangung der Daten, spätestens **binnen eines Monats**

6. BETROFFENENRECHTE

BETROFFENENRECHTE (1)

- Recht auf Auskunft
  ua. die konkret verarbeiteten Daten, Datenkopien, Verarbeitungszwecke, Empfänger, Speicherfrist, Herkunft der Daten,…
- Recht auf Berichtigung
- Recht auf Löschung ("Vergessenwerden")
  zB wenn Daten für Zwecke nicht mehr notwendig, bei Widerruf der Einwilligung, bei unrechtmäßiger Verarbeitung



BETROFFENENRECHTE (2)

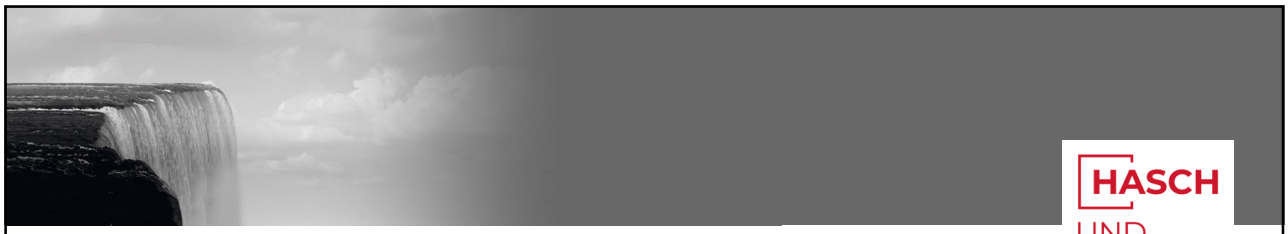
- Recht auf Datenübertragbarkeit (Übermittlung in gängigem maschinenlesbaren Format)
- Betroffene sollen die Möglichkeit haben bspw. leicht einen Anbieter zu wechseln → daher wichtig, dass erforderliche Daten in gängigem Format zur Verfügung stehen

BETROFFENENRECHTE (3)

- Recht auf Intervention bei automatisierten Entscheidungen ("Profiling")

  ⇨ zB Kreditwürdigkeit, die automatisiert erfolgt

  Betroffene haben Recht auf manuelle Prüfung (= Intervention)



BETROFFENENRECHTE – FRIST

- Verantwortliche müssen auf Auskunfts-, Richtigstellungs-, Löschungs-, Datenübertragungs- und Widerspruchsbegehren
  - grundsätzlich unverzüglich
  - jedenfalls aber innerhalb 1 Monats reagieren
  - im Ausnahmefall, wenn viele und komplexe Anfragen vorliegen, ist die Frist auf 2 Monate verlängerbar
- Auskünfte sind unentgeltlich zu erteilen

7. AUFTRAGSVERARBEITER

AUFTRAGSVERARBEITER

- natürliche oder juristische Person, die Daten im Auftrag des Verantwortlichen verarbeitet
- verarbeitet Daten nicht für eigene Zwecke, sondern zur Durchführung des Auftrages des Verantwortlichen
- ist rechtlich eigenständig

EINSATZ VON AUFTRAGSVERARBEITERN (1)

- sorgfältige Auswahl des Auftragsverarbeiters
  Art 28 Abs 1 DSGVO: AV muss hinreichende Garantien für geeignete technische und organisatorische Maßnahmen, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der Betroffenen gewährleistet, bieten.
- schriftlicher Auftragsverarbeitervertrag erforderlich
- Datenverarbeitung auf Weisung des Verantwortlichen

EINSATZ VON AUFTRAGSVERARBEITERN (2)

- Verantwortlicher bestimmt Zweck und Mittel der Verarbeitung
  Sobald dies durch den AV erfolgt, wird dieser zum Verantwortlichen
- Datenweitergabe an AV innerhalb der EU zulässig
  (ohne gesonderte Rechtsgrundlage)

INHALTE DES AUFTRAGSVERARBEITERVERTRAGES (1)

- Weisungsgebundenheit
- Mitarbeiterbelehrung, Verpflichtung der Mitarbeiter zur Vertraulichkeit (Datengeheimnis § 6 DSG)
- Datensicherheitsmaßnahmen
- Voraussetzungen für Beiziehung von Sub-Auftragsverarbeitern
- Unterstützungspflicht hins. Betroffenenrechte

INHALTE DES AUFTRAGSVERARBEITERVERTRAGES (2)

- Maßnahmen bei Beendigung der Auftragsverarbeitung
  Löschung/Rückgabe der Daten
- Informationspflicht (hins. Überprüfungspflicht des Verantwortlichen)

HAFTUNG DES AUFTRAGSVERARBEITERS (1)

- Verantwortlicher ist für Einhaltung des Datenschutzrechts verantwortlich
- mögliche Haftung des AV aufgrund Mitverschuldens bei Unterlassung gesetzlicher oder vertraglicher Sorgfaltspflichten
  (insbes. Datensicherheit: technische und organisatorische Maßnahmen)

HAFTUNG DES AUFTRAGSVERARBEITERS (2)

- Auftragsverarbeiter haftet insbes. bei Nichteinhaltung der gesetzlichen oder vertraglichen Pflichten oder bei Nichtbefolgung der Weisungen des Verantwortlichen (Schadenersatz und Verwaltungsstrafe, Haftung im Regressweg für Strafen des Kunden)
- Warnpflicht des AV an den Verantwortlichen, wenn Weisung gegen DSGVO verstößt

HAFTUNG DES AUFTRAGSVERARBEITERS (3)

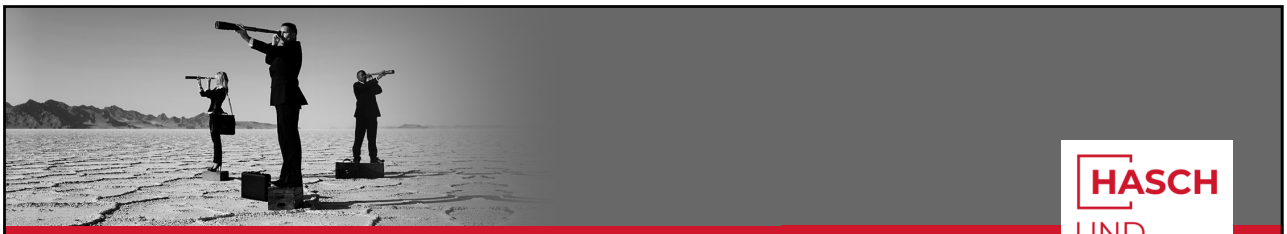
- **Haftung für Vertraulichkeit/Verschwiegenheit:**
  Gemäß Art 28 Abs 3 lit b) DSGVO muss der Auftragsverarbeiter gewährleisten, dass alle mit der Datenverarbeitung befassten Personen zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen
  ⇨ mögliche Haftung des AV wegen unterlassener **Vertraulichkeitsverpflichtung** und Belehrung über das **Datengeheimnis**

HAFTUNG DES AUFTRAGSVERARBEITERS (4)

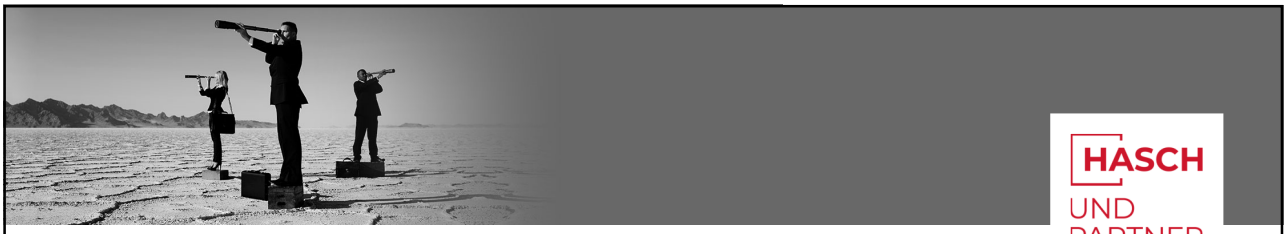
- **Haftung bei mangelnder Datensicherheit:**
  Gemäß Art 28 Abs 3 lit c) DSGVO muss der Auftragsverarbeiter die erforderlichen und vereinbarten technischen und organisatorischen Maßnahmen ergreifen (Haftung bei Unterlassung dieser Maßnahmen)

HAFTUNG DES AUFTRAGSVERARBEITERS (5)

- Haftung bei **unterlassener Data Breach Notification**:
  gemäß Art 28 Abs 3 lit f) DSGVO muss der AV seinen Kunden **unverzüglich** von Verletzung des Schutzes personenbezogener Daten informieren, damit der Kunde als Verantwortlicher der Meldeverpflichtung an die Datenschutzbehörde **binnen 72 Stunden** nachkommen kann
- Bei **unterlassener/verspäteter Meldung**:
  Kunde erhält ggf. Strafe bzw. muss Schadenersatz leisten an Betroffene ⇨ **Regress** gegenüber Auftragsverarbeiter

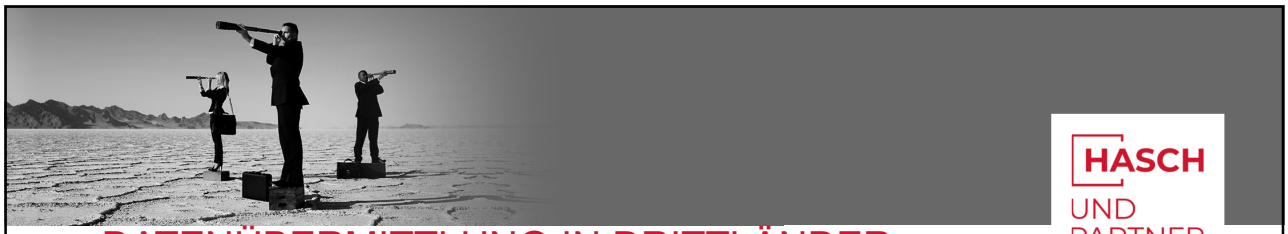


8.
DATENÜBERMITTLUNG IN DRITTLÄNDER



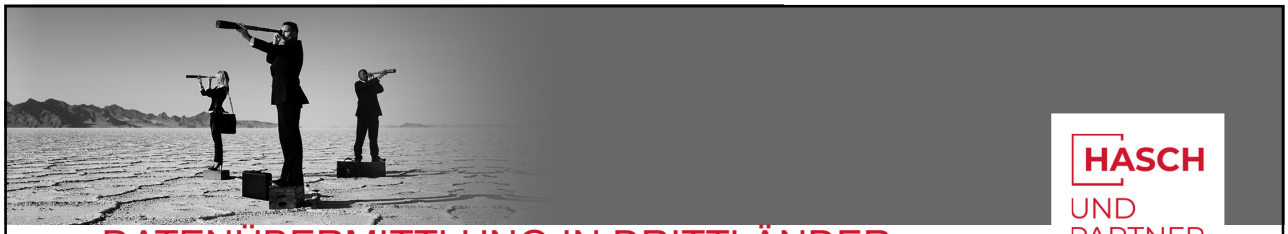
DATENÜBERMITTLUNG IN DRITTLÄNDER

- Drittland = jedes Land außerhalb des EWR
- Zulässigkeitsvoraussetzungen in Art 44ff DSGVO geregelt
- Sicherzustellen, dass das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird



DATENÜBERMITTLUNG IN DRITTLÄNDER ZULÄSSIGKEITSVORAUSSETZUNGEN (1)

- **Angemessenheitsbeschluss** der EU-Kommission dzt. zB für Kanada, Israel, Japan, Neuseeland, Südkorea, UK; **nicht:** USA
- Garantien: insbes. **Standardvertragsklauseln** (SCC), ggf. mit zusätzlichen Schutzmaßnahmen
- Ausdrückliche **Einwilligung** der Betroffenen
- Erforderlichkeit zur **Vertragserfüllung** zwischen Verantwortlichem und Betroffenem



DATENÜBERMITTLUNG IN DRITTLÄNDER ZULÄSSIGKEITSVORAUSSETZUNGEN (2)

- Wichtige Gründe **öffentlichen Interesses**
- Erforderlichkeit zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen**
- Schutz **lebenswichtiger Interessen**
- Übermittlung aus **öffentlichem Register**

PROBLEMFALL USA – SCHREMS II (1)

Bis 2020 **Privacy Shield:**

- Vereinbarung zwischen USA und EU über Grundsätze zum Datenschutz
- an US-Unternehmen, die sich dem Privacy Shield unterwarfen (Selbstverpflichtung), durften Daten aufgrund eines **Angemessenheitsbeschlusses** übermittelt werden

PROBLEMFALL USA – SCHREMS II (2)

- durch **EUGH** im Juli 2020 für **ungültig** erklärt ("Schrems II")
  ⇨ USA gewährleisten kein angemessenes Schutzniveau, da US-Behörden in unverhältnismäßiger Weise auf Daten zugreifen und diese verwenden können

PROBLEMFALL USA – SCHREMS II (3)

- **Standardvertragsklauseln** weiterhin gültig in Bezug auf USA, jedoch **nur mit zusätzlichen Maßnahmen und Garantien**
- zusätzl. Garantien/Maßnahmen:
  - **Transfer Impact Assessment:** Prüfung und Dokumentation, ob beim Datenimporteur angemessenes Datenschutzniveau sichergestellt werden kann
  - **Informations- und Abwehrpflichten** des Datenimporteurs bei Behördenzugriffen
- FAZIT: **Rechtssicherer Datentransfer in USA kaum möglich**

9.
DAS DATENGEHEIMNIS

Verpflichtung der Mitarbeiter

DAS DATENGEHEIMNIS - § 6 DSG (1)

Auszug aus § 6 Datenschutzgesetz:

(1) Der **Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter** – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – **haben personenbezogene Daten** aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, **geheim zu halten**, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

DAS DATENGEHEIMNIS - § 6 DSG (2)

(2) **Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln**. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

DAS DATENGEHEIMNIS - § 6 DSG (3)

(3) Der **Verantwortliche und der Auftragsverarbeiter** haben die von der Anordnung betroffenen **Mitarbeiter** über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu **belehren**.

DATENGEHEIMNIS (1)

- berufsmäßig bekannte personenbezogene Daten sind geheim zu halten
- Mitarbeiter sind schriftlich zur Einhaltung des Datengeheimnisses zu verpflichten (sofern sich dies nicht bereits aus dem Gesetz ergibt)
- Insbesondere sind die Mitarbeiter über die Folgen einer Verletzung des Datengeheimnisses zu belehren!

DATENGEHEIMNIS (2)

- unmittelbare gesetzliche Verpflichtung der Mitarbeiter
- bei Verstößen sind Geldstrafen (zB § 62 DSG) und Schadenersatzklagen möglich
- Strafen bis zu EUR 50.000,00

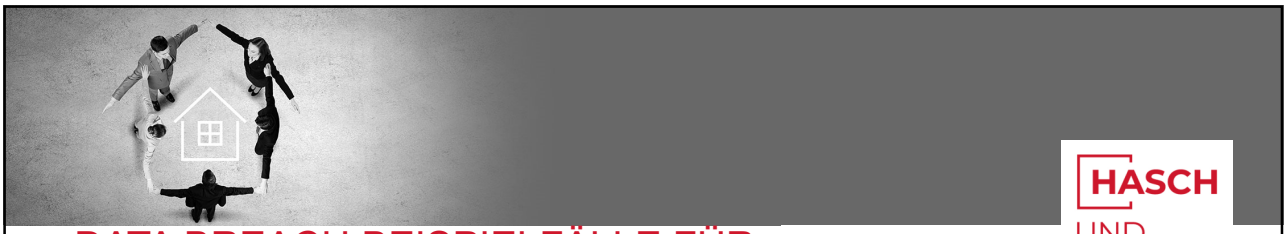
10.
DATENSCHUTZVERLETZUNGEN UND RECHTSFOLGEN

DATA BREACH

- "Data Breach" = Verletzung des Schutzes personenbezogener Daten
- Meldung an Datenschutzbehörde erforderlich
- Ausnahme: keine Gefahr für betroffene Person(en) (Risikoeinschätzung)
- zusätzlich ggf. Mitteilung an betroffene Person(en) erforderlich

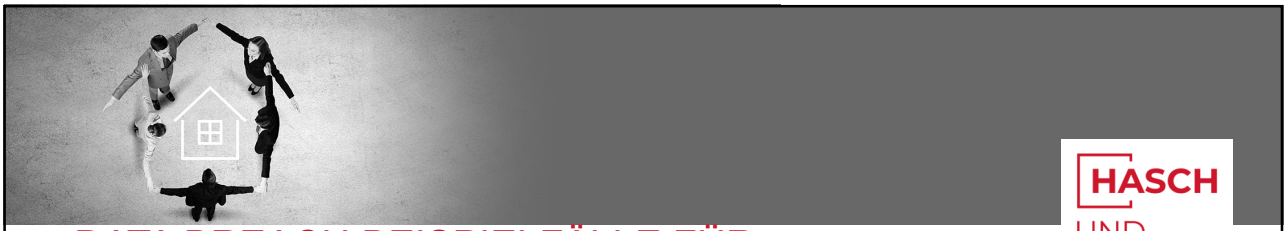
DATA BREACH / RISIKOEINSCHÄTZUNG

- Art der Datenschutzverletzung
- Art, Sensibilität und Umfang personenbezogener Daten
- Identifizierbarkeit betroffener Personen
- möglichen Konsequenzen und Auswirkungen
- Zahl der betroffenen Personen



DATA BREACH BEISPIELFÄLLE FÜR MELDEPFLICHT (1)

- falsche Adressierung, Versendung von Nachrichten/E-Mails an falschen Empfänger
- Gezielte Angriffe durch Dritte, zB Hackerangriffe, Phishingattacken, Zugriffe durch nicht befugte Personen
- Verlorengegangene oder gestohlene Notebooks, Datenträger oder Unterlagen



DATA BREACH BEISPIELFÄLLE FÜR MELDEPFLICHT (2)

- Aufdeckung von Passwörtern
- ungewollte Veröffentlichung personenbezogener Daten (etwa durch technische Fehler)
- Einbruch in Serverraum (ggfs mit Verlust der Back-Up-Speichermedien)

DATA BREACH – INHALT DER MELDUNG (1)

- Art der Verletzung;
- betroffene Datenkategorien;
- ungefähre Zahl der betroffenen Personen;
- ungefähre Zahl der betroffenen personenbezogenen Datensätze;

DATA BREACH – INHALT DER MELDUNG (2)

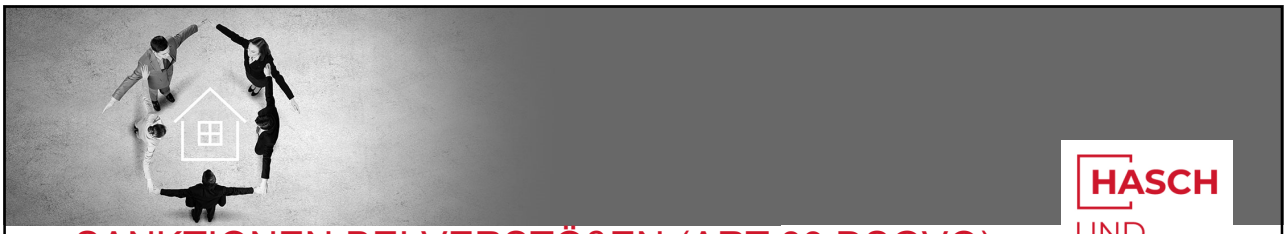
- Name und Kontaktdaten der Anlaufstelle (bzw. des Datenschutzbeauftragten);
- Beschreibung der wahrscheinlichen Folgen;
- Beschreibung der ergriffenen Maßnahmen zur Behebung der Datenpanne und ihrer Folgen

DATA BREACH – MELDUNG (1)

- **Frist** für die **Meldung an die Datenschutzbehörde**: unverzüglich, maximal binnen **72 Stunden**
- Geldstrafen bei unterlassener oder verspäteter Meldung
- Dokumentation der Verletzungen und der ergriffenen Maßnahmen!

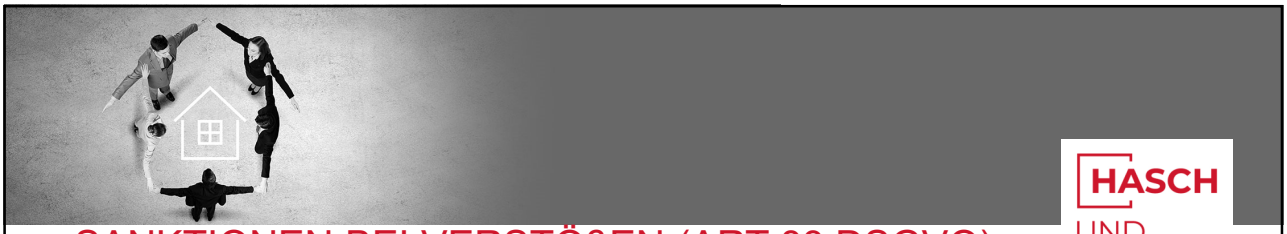
DATA BREACH – MELDUNG (2)

- Zusätzlich zur Behördenmeldung ggf. **Benachrichtigung der Betroffenen**:
  - unverzüglich
  - wenn hohes Risiko für Betroffene
  - in Ausnahmefällen keine Benachrichtigung erforderlich (zB bei nachfolgenden Maßnahmen zur Risikominimierung)



SANKTIONEN BEI VERSTÖßEN (ART 83 DSGVO) (1)

- Geldbußen durch Datenschutzbehörde, subsidiär Verwaltungsstrafen
- Strafrahmen bis **EUR 10 Mio** oder **2 % des Jahresumsatzes:**
  bei Verstoß gegen Bestimmungen bezüglich
  - Datenschutz durch Technikgestaltung
  - Auftragsdatenverarbeitung
  - Verzeichnis von Verarbeitungstätigkeiten
  - Datensicherheit/Datenschutzfolgenabschätzung



SANKTIONEN BEI VERSTÖßEN (ART 83 DSGVO) (2)

- Strafrahmen bis **EUR 20 Mio** oder **4 % des Jahresumsatzes:**
  bei Verstoß gegen
  - Betroffenenrechte
  - Bestimmungen über den internationalen Datenverkehr
  - die Grundsätze rechtmäßiger Datenverarbeitung

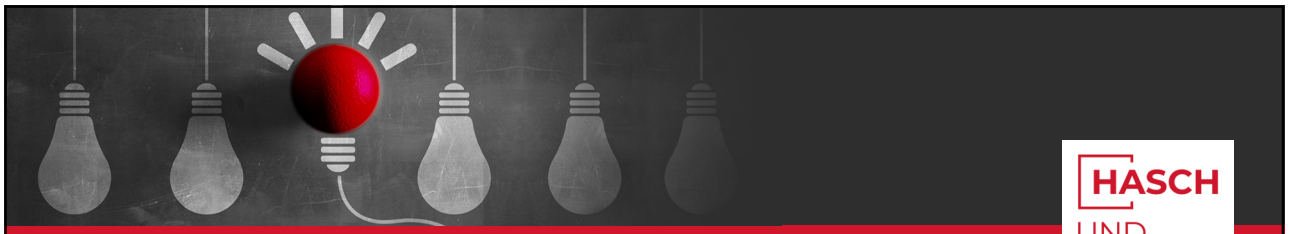
RECHTSFOLGEN BEI VERSTÖßEN (1)

Neben Geldbußen drohen bei Verletzungen des Datenschutzrechts auch **zivilrechtliche Ansprüche**, etwa

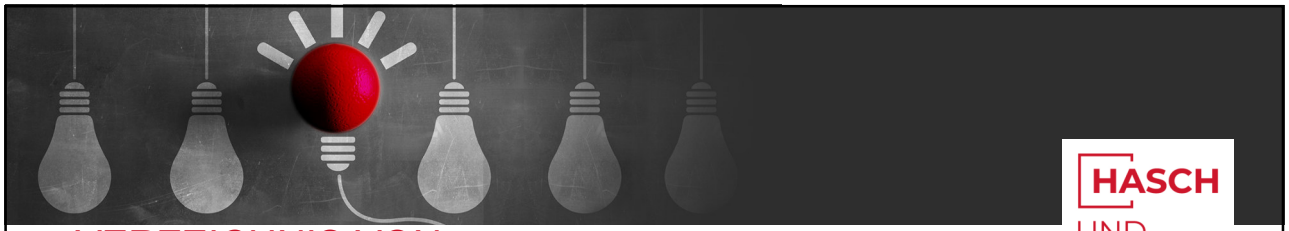
- Schadenersatzansprüche von Betroffenen (auf für immaterielle Schäden)
- Schadenersatzansprüche/Regressansprüche von Verantwortlichen gegenüber Auftragsverarbeiter
- Unterlassungsansprüche von Mitbewerbern nach UWG (gestützt auf Wettbewerbsvorsprung durch Rechtsbruch)
- Verbandsklagen

RECHTSFOLGEN BEI VERSTÖßEN (2)

- Die Strafen können gegen die juristische Person oder deren Verantwortlichen (Geschäftsführer, verantwortlicher Beauftragter) verhängt werden. Die Behörde hat jedoch von der Bestrafung der natürlichen Person abzusehen, wenn für dasselbe Vergehen bereits eine Strafe gegen das Unternehmen verhängt wurde.



11.
DATENVERARBEITUNGSVERZEICHNIS



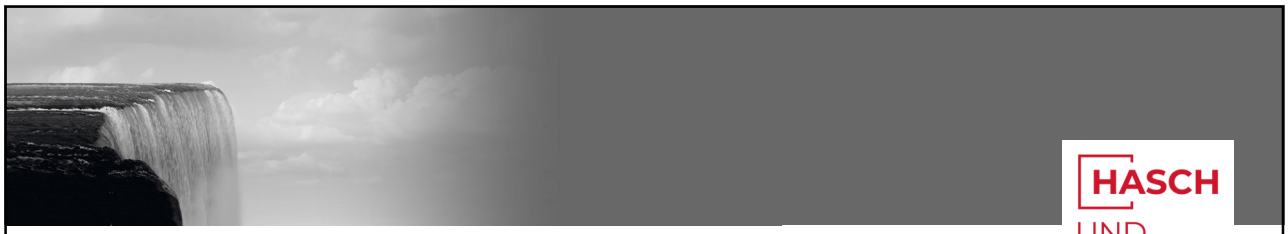
VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

- Unternehmen müssen Verzeichnis aller Verarbeitungstätigkeiten führen
- Verantwortliche und Auftragsverarbeiter sind dazu verpflichtet
- Art 30 Abs 5 DSGVO Ausnahmen

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN INHALTE:

- Name und Kontaktdaten
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und Daten
- Löschfristen
- Kategorien von Empfängern
- Übermittlung in Drittstaaten und internationale Organisationen
- Beschreibung Sicherheitsmaßnahmen

12. DATENSCHUTZFOLGENABSCHÄTZUNG

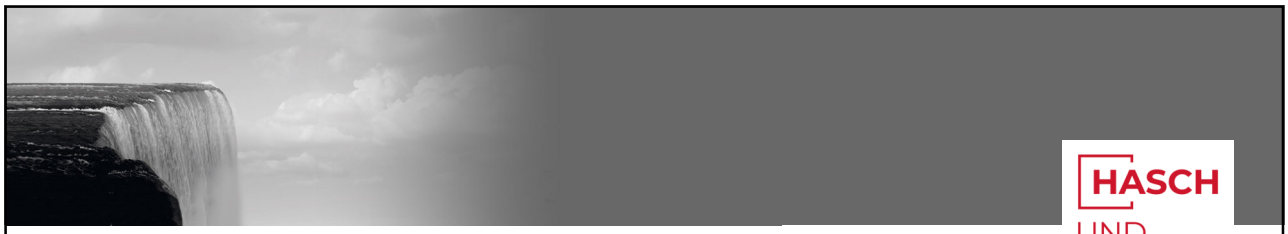


DATENSCHUTZ-FOLGENABSCHÄTZUNG (1)

- Schwellwertanalyse
  - Bewertung oder Einstufung der Betroffenen (zB Profiling)?
  - automatisierte Entscheidungsfindung?
  - systematische Überwachung öffentlich zugänglicher Bereiche?
  - vertrauliche oder höchst persönliche Daten?

DATENSCHUTZ-FOLGENABSCHÄTZUNG (2)

- Großer Umfang?
- Kombination, Abgleichung oder Zusammenführung der Datensätze über die vernünftigen Erwartungen der Betroffenen hinaus?
- Besonders schutzbedürftige Personen (zB Kinder?)
- neue Technologien oder innovative Lösungen?
- Wird die Ausübung von Betroffenenrechten verhindert?

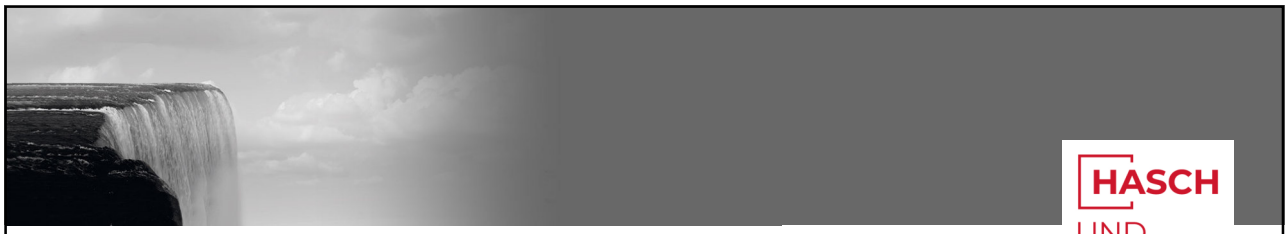


DATENSCHUTZ-FOLGENABSCHÄTZUNG (3)

- Black-List-Österreich:
  - Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V)
  - Bewertung oder Einstufung natürlicher Personen
  - Überwachung natürlicher Personen
  - Zusammenführen oder abgleichen von Datensätzen

DATENSCHUTZ-FOLGENABSCHÄTZUNG (4)

- White-List-Österreich:
  - Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV)
  - Kundenverwaltung
  - Personalverwaltung
  - Zutrittskontrollsysteme
  - Bild- und Akustikverarbeitung in Echtzeit



DATENSCHUTZ-FOLGENABSCHÄTZUNG (5)

- Risikoanalyse
- folgt idR auf Schwellwertanalyse

13.
DER DATENSCHUTZBEAUFTRAGTE

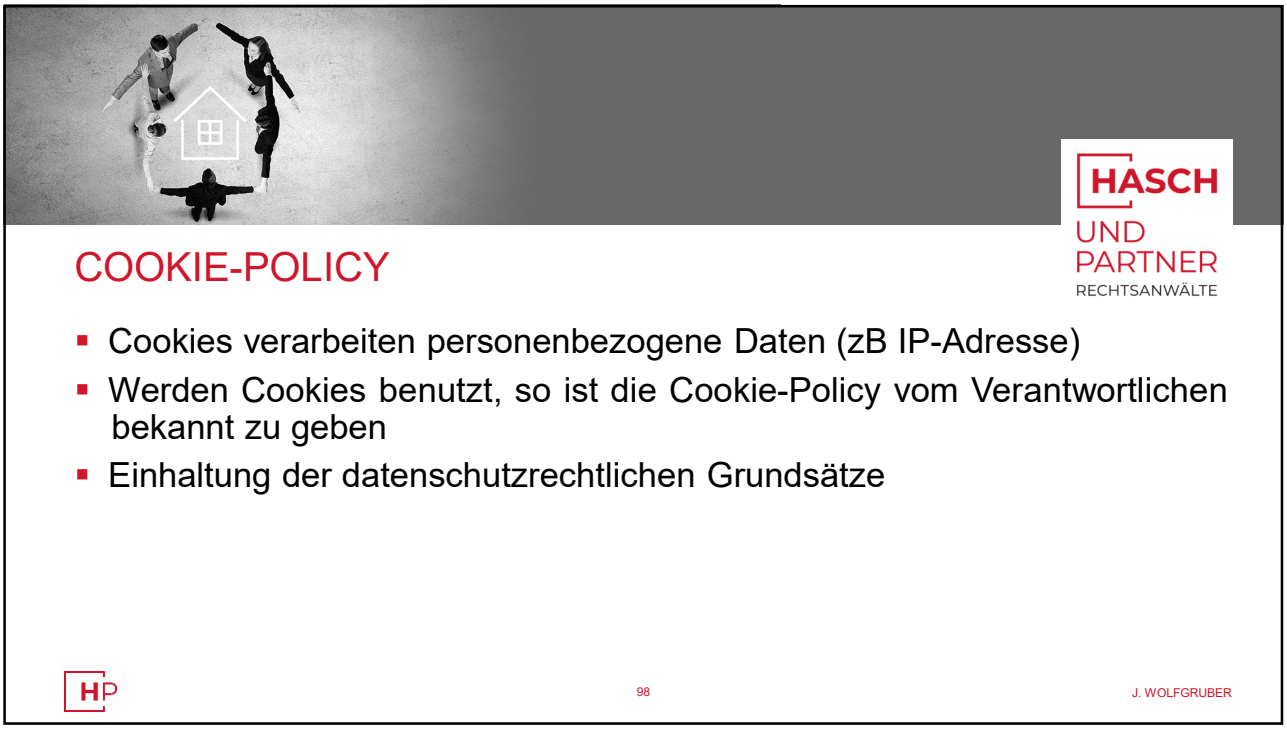
DATENSCHUTZBEAUFTRAGTER (1)

- Aufgaben eines Datenschutzbeauftragten:
  - Beratung der Verantwortlichen bzw. der Auftragsverarbeiter
  - Kombination Branchenwissen mit Datenschutzrecht
  - Überwachung und Überprüfung
  - Berichtspflicht Managementebene
  - Weisungsfrei

DATENSCHUTZBEAUFTRAGTER (2)

- Erfordernis eines Datenschutzbeauftragten
  - Behörde oder öffentliche Stelle (Ausnahme bei Gerichten)
  - Kerntätigkeit des Unternehmens besteht in der umfangreichen, regelmäßigen und systematischen Überwachung von betroffenen Personen
  - Die Kerntätigkeit des Unternehmens besteht in der umfangreichen Verarbeitung von sensiblen oder strafrechtlich relevanten Daten.
  - Ein spezifisches europäisches oder nationales Recht schreibt die Benennung verpflichtend vor.

14.
WEITERE AUSGEWÄHLTE ASPEKTE



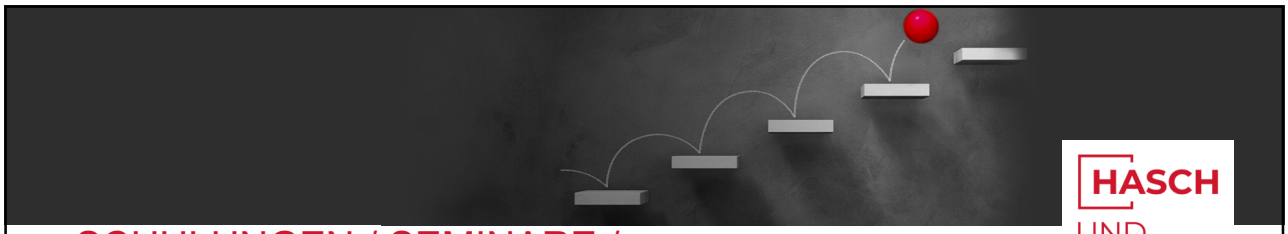
COOKIE-POLICY

- Cookies verarbeiten personenbezogene Daten (zB IP-Adresse)
- Werden Cookies benutzt, so ist die Cookie-Policy vom Verantwortlichen bekannt zu geben
- Einhaltung der datenschutzrechtlichen Grundsätze

DIREKTWERBUNG

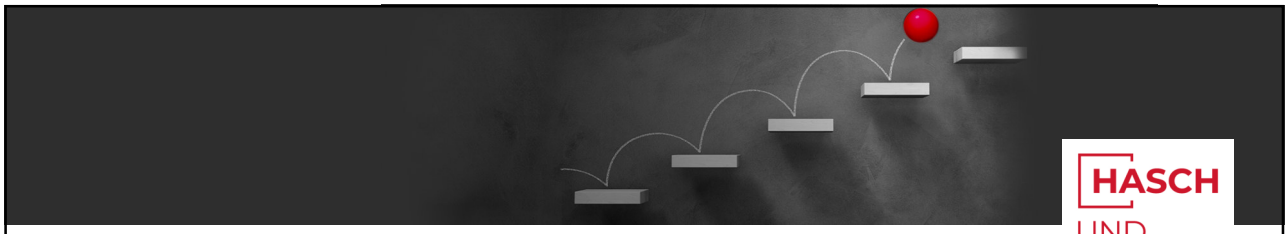
- Geregelt in § 174 TKG (früher § 107 TKG)
- Unerbetene Anrufe / Nachrichten (Direktwerbung) unzulässig.
- Nutzer kann jedoch einwilligen
- Auch Influencer Marketing kann verbotene Direktwerbung sein!

15.
COMPLIANCE UMSETZUNG



SCHULUNGEN / SEMINARE / VERHALTENSKODEX

- Schulungen
- Seminare
- Verhaltenskodex



PRAXISTIPPS

- Datenschutzbeauftragter? Ja/Nein?
- Organisation
- Regelmäßige Überprüfung und Anpassung von Verträgen
- Unternehmensrichtlinien und Leitlinien
- Fahrplan Data-Breach

HASCH UND PARTNER RECHTSANWÄLTE

FRAGEN UND ANTWORTEN

HASCH UND PARTNER RECHTSANWÄLTE

FAQ 1

- Jemand hat meinen Newsletter abbestellt, was tun?
  - Aus Verteiler löschen/unter Umständen E-Mail Adresse löschen
- Wie reagiere ich auf ein Auskunftsersuchen?
- Feststellung der Identität ⇨ Ansuchen berechtigt? ⇨ Auskunft erteilen; ACHTUNG FRIST 1 MONAT

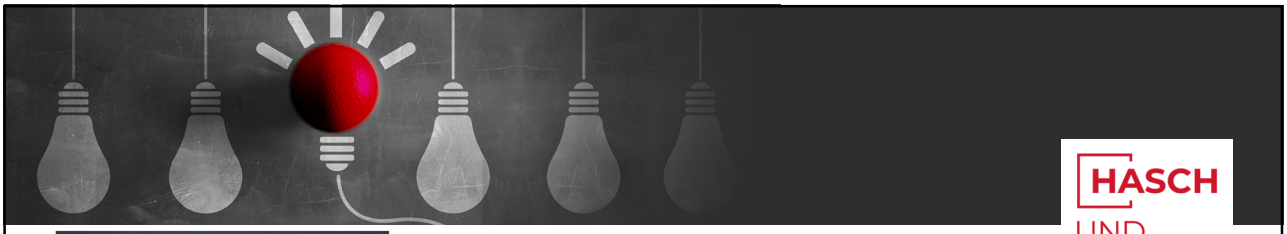
FAQ 2

- Was sind technisch notwendige Cookies?
  - Sitzungsverwaltung
  - Formulareingaben
- Cookies als personenbezogene Daten?
  - Nicht automatisch
  - Im Einzelfall aber durchaus

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

DISCLAIMER

Es wird darauf verwiesen, dass alle Angaben in dieser Unterlage trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung der Autoren ausgeschlossen ist. Diese Unterlage kann eine rechts-freundliche Beratung im Anlassfall nicht ersetzen.



Mag. Johannes Wolfgruber, MBA

Landstraße 47
4020 Linz
Telefon: 0732 / 77 66 44
E-Mail: j.wolfgruber@hasch.eu
www.hasch.eu