Datenschutz

Sechs goldene Regeln

- **Rechtmäßigkeit**
  Gesetz, Einwilligung, Vertrag, Dienst- oder Betriebsvereinbarung
- **Zweckbindung**
  Verwendung nur für Erhebungszweck
- **Datenminimierung und Speicherbegrenzung**
  Verarbeitung nur soweit für Erhebungszweck erforderlich
- **Transparenz und Betroffenenrechte**
  Unterrichtung über Verwendung, Auskunfts-/Berichtigungs-/Löschrechte
- **Datensicherheit und Richtigkeit**
  Technische und organisatorische Maßnahmen, Integrität und Vertraulichkeit
- **Kontrolle**
  Interner / externer Datenschutzbeauftragter; Audit

Zentrale Befugnisnorm (Art. 6 DSGVO)

Datenverarbeitung ist nur (!) rechtmäßig, wenn:

- Einwilligung
- Vertragserfüllung
- Erfüllung rechtlicher Verpflichtung
- Lebenswichtige Interessen
- Ausübung öffentliche Gewalt
- Wahrung berechtigter Interessen (sofern Interessen des Betroffenen nicht überwiegen)

Eckpunkte Einwilligung

- Die Einwilligung muss informiert und freiwillig erfolgen.
- Die Einwilligung muss nicht mehr schriftlich sein.
- Die Einwilligung ist mit Wirkung für die Zukunft widerruflich.

Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher gem. Art. 30 Abs. 1 DSGVO

- Muster-Vorlage der DSK
- Kurzpapier der DSK zum Thema
- Hinweise der DSK

Technisch-organisatorische Maßnahmen Art. 30 Abs. 1 S. 2 lit. g DSGVO

Maßnahmen sind im Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher zu dokumentieren.

- Hinweise dazu in „Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO“ der DSK, Ziffer 6.7
- Standard-Datenschutzmodell
- Leitlinien und Orientierungshilfen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und der Artikel-29-Arbeitsgruppe
- bestehende nationale und internationale Standards (BSI-Grundschutz, ISO-Standards…)

Ist bei der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zu erwarten, hat die Bestimmung der Maßnahmen bereits im Rahmen einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO zu erfolgen.

Anonymität

- Positionspaper BfDI

Datenschutzbeauftragter

- Darf keinen Interessenkonflikt haben, sonst Bußgeld.[1)]

Übermittlung pbD an Drittländer

Ohne weitere über die Rechtsgrundlage für die Übermittlung von pbD hinausgehende Rechtsgrundlage ist die Übermittlung in Länder der EU und Länder des EWR gem. Art. 1 Abs. 3 DSGVO zulässig.

Eine Übermittlung von pbD in Drittländer erfordert neben der Rechtmäßigkeit der Verarbeitung (nach Art. 6 Abs. 1 und Art. 9 Abs. 2 DSGVO) eine zusätzliche Legitimation (Art. 44 ff. DSGVO):

- Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO)
- geeignete Garantien und den betroffenen Personen zustehende durchsetzbare Rechte und wirksame Rechtsbehelfe (Art. 46 DSGVO)
    - Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules (BCR)) (Art. 47 DSGVO)
    - Standarddatenschutzklauseln
    - genehmigte Verhaltensregeln (Art. 40 DSGVO)
    - genehmigter Zertifizierungsmechanismus (Art. 42 DSGVO)
    - genehmigte Vertragsklauseln
- Ausnahmen in bestimmten Fällen (Art. 49 DSGVO)
    - ausdrückliche Einwilligung der betroffenen Person, nach Info über mögliche Risiken (Art. 49 Abs. 1 lit. a DSGVO)

    - Erfüllung eines Vertrages mit der betroffenen Person bzw. vorvertragliche Maßnahmen auf Antrag der etroffenen Person (Art. 49 Abs. 1 lit. b DSGVO)
    - Abschluss oder Erfüllung eines Vertrages im Interesse der betroffenen Person (Art. 49 Abs. 1 lit. c DSGVO)
    - wichtige Gründe des öffentlichen Interesses, die im Unionsrecht oder dem Recht des Mitgliedstaates anerkannt sind (Art. 49 Abs. 1 lit. d i.V.m. Art. 49 Abs. 4 DSGVO)
    - die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 49 Abs. 1 lit.e DSGVO)
    - der SChutz lebenswichtiger Interessen, sofern die betroffene Person außerstande ist ihre Einwilligung zu geben (Art. 49 Abs. 1 lit. f DSGVO)
    - die Übermittlung aus einem Register, das zur Information der Öffentlichkeit bestimmt ist (Art. 49 Abs. 1 lit. g DSGVO)
- Einmalige Übermittlung gem. Art. 49 Abs. 1 S. 2 DSGVO

Der Angemessenheitsbeschluss für die USA bzw. den EU-US-Privacy-Shield, eine Form der freiwillgigen Selbstzertifizierung für Organisationen wurde zum 16.7.2020 für ungültig erklärt. Der EU-Privacy-Shield stellt somit keine Legitimation für Übermittlungen pbD in die USA mehr dar! Gemäß einer repräsentativen Umfrage des Digitalverbandes Bitkom stützen sich 91 % der befragten Organisationen auf Standardvertragsklauseln

[1)]

vgl. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2022/20220920-BlnBDI-PM-Bussgeld-DSB.pdf.

From:
https://gesunde-vernetzung.de/ - **DigHealthWiki**

Permanent link:
https://gesunde-vernetzung.de/doku.php?id=dighealth:div:ds&rev=1664454888

Last update: **2022/09/29 12:34**