What‘s new, tin foil hat?

Die Europäische Datenschutz-Grundverordnung

Grundgesetz (GG) seit 1949

Art. 1 I, 2 I GG: Allgemeines Persönlichkeitsrecht, Recht am eigenen Bild, am eigenen Wort

BVerfG 1983: GR auf informationelle Selbstbestimmung (RiS)

BVerfG 2008: GR auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme

Art. 3 GG Gleichheitsgrundsatz

Art. 5 GG: Meinungsfreiheit, Informations- u. Pressefreiheit

Art. 10 GG: Telekommunikationsgeheimnis

Sonstige Grundrechte: Beruf, Wohnung, Familie, Religion, Eigentum

Art. 19 IV GG: Rechtsschutzgarantie

Art. 20 GG: Sozialstaatsprinzip

Europäische Grundrechte-Charta (GRCh) 2009

Art. 6 Jeder Mensch hat Recht auf Freiheit und Sicherheit

Art. 7 Achtung von Privatsphäre, Familie, Wohnung, Kommunikation

Art. 8 Recht auf Datenschutz (Zweckbindung, Auskunft, unabhängige Kontrolle)

Art. 11 Meinungs- und Informationsfreiheit

Art. 20 ff Gleichheit u. Diskriminierungsverbot,

Art. 27 ff. Solidarität/Arbeitnehmerrechte

Art. 31 Abs. 1: „Jeder Arbeitnehmerin und jeder Arbeitnehmer hat das Recht auf gesunde, sichere und würdige Arbeitsbedingungen.“

Art. 44 Petitionsrecht, Art. 47 Rechtsschutz

Entwicklung der Datenschutzgesetze

Seit 1970 Landesdatenschutzgesetze

Seit 1976 Bundesdatenschutzgesetz

BVerfG 1983: Gesetzesvorbehalt bei informationelle Eingriffen

1996 Europäische Datenschutzrichtlinie (EG-DSRl)

2001: Umsetzung EG-DSRl

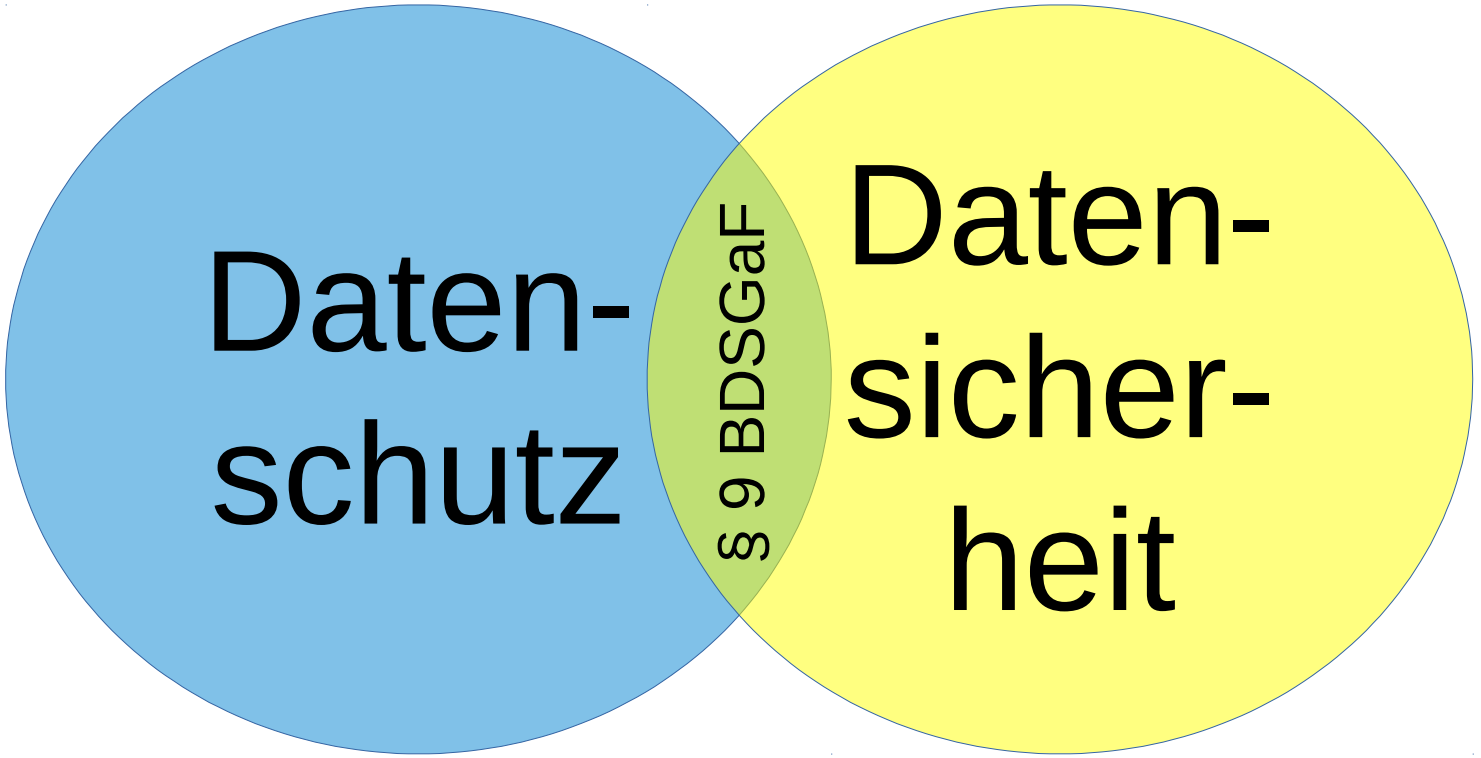
Seit 80er Jahre: Versprechen eines ArbeitnehmerDSGesetzes

2009: BeschäftigtenDSRegelung (§ 32 BDSG) nach Skandalen

2016/Mai 2018: Europäische Datenschutz-Grundverordnung (DSGVO)

2017/Mai 2018: BDSG-neu

Datenschutz vs Datensicherheit



„Personenbezogene Daten“ Art. 4 DSGVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1) „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen;

„Verarbeiten“
Art 4 DSGVO

2) „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das **Erheben**, das **Erfassen**, die **Organisation**, das **Ordnen**, die **Speicherung**, die **Anpassung** oder **Veränderung**, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

7 Regeln des Datenschutzes

1) **Rechtmäßigkeit** (Art. 5 ff. EG-DSRl, § 4 BDSGaF, Art. 5 ff. DSGVO)
2) **Einwilligung** (Art. 7 lit. a EG-DSRl, § 4a BDSGaF, Art. 7 DSGVO)
3) **Zweckbindung** (Art. 6 I EG-DSRl, §§ 28 ff. BDSGaF; Art. 5 I lit. b DSGVO)
4) **Erforderlichkeit** und **Datensparsamkeit** (Art. 6 I c, e EG-DSRl, § 3a BDSGaF, Art. 5 I lit. c, e DSGVO)
5) **Transparenz** und **Betroffenenrechte** (Art. 11 ff. EG-DSRl, § 33 ff. BDSGaF, Art. 12 ff. DSGVO)
6) **Datensicherheit** (Art. 17 I EG-DSRl, § 9 BDSGaF, Art. 25, 32 DSGVO)
7) **Kontrolle** (Art. 28 EG-DSRl, § 38 BDSGaF, Art. 51 ff. DSGVO)

Einwilligung Art. 7 DSGVO

1) Einwilligung nachweisen können
2) Wenn schriftlich, in klarer, verständlicher Sprache
3) Kann jederzeit widerrufen werden
4) War der erfasste Datenumfang wirklich nötig, oder wurde die betroffene Person überrumpelt?

§ 32 BDSG-alt

(1) Personenbezogene Daten eines Beschäftigten dürfen für **Zwecke des Beschäftigungsverhältnisses** erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur **Aufdeckung von Straftaten** dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) Die **Beteiligungsrechte der Interessenvertretungen** der Beschäftigten bleiben unberührt.

Europäischer Rahmen BeschäftigtenDS

1995 EG-DSRl enthält keine Aussagen

2001/2002 EU-Konsultation zum Arbeitnehmerdatenschutzrecht

Bisher nur wenige nationale Normierungen

2009 Art. 8 EuGRCharta: Grundrecht auf Datenschutz, § 32 BDSG-alt

Seit Anfang 2012 EU-DSGVO, Inkrafttreten 25.05.2016, direkte Anwendbarkeit 25.05.2018

Art. 88 DSGVO, nationale Konkretisierung § 26 BDSG-neu

Ziele der DSGVO

Einheitliche verbindliche Regelungen

Marktortprinzip

One-Stop-Shop (eine zuständige Aufsicht)

Transparenz für Betroffene

Privacy by Design/Privacy by Default

Risikofolgenabschätzung

Verbindlicher und rechtssicherer Drittland-Datentransfer

Verbesserungen bei Beschwerden und Rechtsschutz

Wirksame Sanktionen

Weitere Neuerungen

- Recht auf Vergessenwerden
- Recht auf Datenübertragbarkeit (als Schutz for walled Gardens)
- Widerspruch bei automatisierten Einzelfallentscheidungen

Grundprinzipien der DSGVO (Art. 5 Abs. 1)

a) Rechtmäßigkeit, Treu und Glauben, Transparenz

b) Zweckbindung

c) Datenminimierung / Erforderlichkeitsgrundsatz

d) Richtigkeit

e) (zeitliche) Speicherbegrenzung

f) Integrität und Vertraulichkeit

Art. 5 Abs. 2: Verantwortlichkeit - Rechenschaftspflicht

Rechtmäßigkeit d. Verarbeitung (Art. 6 Abs. 1)

a) Einwilligung (→ Art. 7, 8)

b) Vertragsabwicklung

c) Erfüllung rechtlicher Verpflichtungen

d) Schutz lebenswichtiger Interessen

e) Wahrnehmung öffentlicher Interessen durch öffentliche Stellen

f) Wahrnehmung berechtigter Interessen, die gegenüber schutzwürdigen Interessen überwiegen

Verarbeitung sensitiver Daten

Art. 4 Nr. 13-15 Definition Genetische Daten, Biometrische Identifikationsdaten, Gesundheitsdaten

Art. 7 Einwilligung ohne spez. Regelung zu sensiblen Daten, Abs. 4 Keine Freiwilligkeit bei Abhängigkeit zu Vertrag ohne Erforderlichkeit

Art. 9 Abs. 1 Verarbeitungsverbot zu Rasse/Ethnie, Politik, Religion, Gewerkschaft, Genetik, biometrische Identifikation, Gesundheit, Sexualleben

Art. 9 Abs. 2 Zehn Erlaubnistatbestände (von **A**rbeitsR bis Statistik**z**wecke)

Art. 9 Abs. 3 Öffnungsklausel für Berufsgeheimnisse

Art. 90 Öffnungsklausel: Freistellung von Auskunft und Kontrolle bei Berufsgeheimnispflicht

Art 9, Abs 2: Erlaubnistatbestände

a) Ausdrückliche Einwilligung

b) Erforderlich nach Arbeitsrecht, Recht der sozialen Sicherheit oder Sozialschutz

c) Lebenswichtige Interessen

d) Mitgliederverwaltung gemeinnütziger Organisationen

e) Öffentliche Daten

f) Gerichtsverfahren

g) Öffentliches Interesse

h) Gesundheitsvorsorge oder Arbeitsmedizin

i) Öffentliches Interesse der Gesundheitsvorsorge

j) Archivzwecke, Forschung

Datenschutz in Unternehmen als fortlaufender Prozess

https://www.heise.de/select/ct/

Art. 88 Verarbeitung Beschäftigtendaten

Nationale Normierung

Gesetz oder Kollektivvereinbarung

Zwecke: Einstellung, Arbeitsvertrag, rechtliche Pflichten, Management, Planung, Organisation, Soziales, Gesundheit, Sicherheit, Arbeitgeber- und Kundenschutz

Rahmen: Menschenwürde, berechtige Interessen, Grundrechte, Transparenz, Übermittlung in der Unternehmensgruppe

Art. 7: Einwilligung nicht ausgeschlossen

Art. 9: Sensitive Daten → Arbeitsrecht und Arbeitsschutz

Inhalte der allgemeinen Datenschutznormen

Abwägung zwischen AN- u. AG-Interessen

aber AG definiert Geschäftsmodell

Absolute Tabuzonen: Kernbereich persönliche Lebensgestaltung, vollständige Persönlichkeitsbilder

Bes. Begründungspflicht und strenge Verhältnismäßigkeitsprüfung: bes. Datenarten, Berufsgeheimnisse, Einwilligung, Einbeziehung arbeitsfremder Daten

Profiling (Art. 4 Nr. 4)

„Profiling“ = jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um **bestimmte persönliche Aspekte**, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu **analysieren oder vorherzusagen**

Automatisierte Einzelfallentscheidung einschließlich Profiling (Art. 22)

(1) Betroffenenrecht, „nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt“

(2) Ausnahmen: Abschluss u. Erfüllung v. Vertrag, Rechtsvorschrift, explizite Einwilligung

(3) Angemessene Schutzmaßnahmen sind nötig (incl. Eingreifen einer Person u. Darlegung d. eigenen Standpunkts, Entscheidungsanfechtg.)

(4) Verbot bzgl. sensitiver Daten, wenn keine angemessenen Maßnahmen gemäß Art. 9 Abs. 2

Angemessene/geeignete Garantien/Maßnahmen zur Wahrung der Grundrechte u. Betr.interessen

(Geregelt z. B. in Art. 6 I lit. f, 9 II, III)

Materielle Regelungen (Ge- u. Verbote, Zweckbindung)

Prozedurale Maßnahmen (Anhörung, Genehmigung, Veto)

Technisch-organisatorische Vorkehrungen (Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit, Nichtverkettbarkeit, Datenminimierung)

Verarbeitung durch **Fachpersonal mit Berufsgeheimnis**

Technisch-organisatorische Schutzziele

- **Vertraulichkeit** (z. B. Verschlüsselung)
- **Integrität, Authentizität** (z. B. Signatur)
- **Verfügbarkeit** (z. B. Backup, Stromversorgung)
- **Intervenierbarkeit** (Löschen, Sperren, Korrektur)
- **Transparenz, Revisionsfähigkeit** (Protokoll, Dokumentation)
- **Nichtverkettbarkeit** (z. B. Abschottung)

BDSGaF
Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet [...] sind insbesondere Maßnahmen zu treffen, die[...] geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Technisch-organisatorische Sicherungen (Art. 25, 32)

Risikoorientierte Betrachtung (vgl. Datenschutz-Folgenabschätzung, Art. 35)

Pseudonymisierung/Anonymisierung, Verschlüsselung

Sicherung v. Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit

Datenminimierung, Speicherbegrenzung

Regelüberprüfung, Bewertung, Evaluation

Zweckbindungssicherung (Nichtverknüpfbarkeit)

Privacy by Design/Privacy by Default (Voreinstellungen)

Datenschutzmanagement nach DSGVO

Verantwortlichkeit Art. 5 II, 24, 31 (Rechenschaftspflicht, Sicherstellung, Nachweis, Überprüfung, Aktualisierung; Kooperation mit Aufsicht)

Verarbeitungsverzeichnis (Art. 30)

Datenschutz-Folgenabschätzung (Art. 35), evtl. vorherige Konsultation (Art. 36)

Breach Notification, Art. 33, 34

Zertifizierung, Art. 42

Datenschutzbeauftragter (DSB), Art. 37-39

DSB-Benennung (Art. 37 I DSGVO, § 38 I BDSG-neu)

Kontrovers in der EU: u. a. mind. 250 Beschäftigte, mind. 5.000 Betroffene

- öffentliche Stelle
- bei umfangreicher regelmäßiger u. systematischer Überwachung (auch AG)
- bei umfangreicher systematischer Verarbeitung sensitiver Daten (Art. 9, 10 DSGVO), jeweils „Kerntätigkeit“ = Haupttätigkeit
- bei mindestens 10 Personen in automatisierter Verarbeitung
- bei Datenschutz-Folgenabschätzung (Art. 35 DSGVO)
- bei geschäftsmäßiger DV zur (anonymen) Übermittlung
- Konzern-DSB und koll. DSB öffentl. Stellen sind zulässig (Art. 37 II, III)
- Freiwillig eigener od. Verbands-DSB (Art. 37 IV)

Persönliche Anforderung Datenschutzbeauftragter (DSB, Art. 37 V-VII DSGVO)

- Interner oder externe Bestellung
- Keine Interessenkonflikte (Art. 38 VI 2)
- Qualifikation: Fachwissen im DS-Recht u. DS-Praxis u. bzgl. Aufgaben des DSB
- Veröffentlichung der Kontaktdaten u. geg. Aufsicht

Bei fehlender Fachkunde od. Interessenkonflikt Abberufungsmöglichkeit (bisher § 38 Abs. 5 S. 3 BDSG, künftig § 40 Abs. 5 S. 2 BDSG-neu)

Stellung des DSB (Art. 38 DSGVO)

Einbindung bei allen DS-Fragen (I)

Unterstützungspflicht (materielle u. Informations-Ressourcen, Zugang zur DV) (II)

Weisungsfreiheit, Abberufungsverbot, Benachteiligungsverbot, Berichte gegenüber der Leitung (III); Kündigungsschutz analog § 626 BGB (?)

Beratung von Betroffenen (IV)

Vertraulichkeitsverpflichtung (V) ZeugnisverweigerungsR (§§ 38 II iVm 6 V, VI BDSG-neu, zuvor § 4f VIa BDSGaF)

Nicht zwingend Vollzeit (VI 1)

Stellung zum Betriebsrat bisher ungeregelt, Art. 88 DSGVO würde Regelung ermöglichen, **BetriebsR kann DSB sein**

Aufgaben (Art. 39 DSGVO)

Risikoorientierter Ansatz bzgl. Art, Umfang, Zweck (Art. 39 II)

Unterrichtung u. Beratung von Leitung u. Beschäftigten

Kontrolle, Zuständigkeitszuweisung, Sensibilisierung, Schulung (auch Berufsgeheimnisse → Schweigepflicht § 203 Abs. 2a StGB)

Beratung u. **Überwachung** der Datenschutz-Folgenabschätzung

Zusammenarbeit u. e) Kommunikation mit Aufsichtsbehörde

Etablierung Durchsetzung v. Binding Corporate Rules (Art. 47 II h), Durchführung Zertifizierung (Art. 42), Verarbeitungsverzeichnis (Art. 30), Breach Notification (Art. 33 f.)

Nicht normiert: Tätigkeitsberichte

Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

Voraussetzung: Hohes Risiko für Rechte und Freiheiten

- bei systematischer und umfassender Bewertung persönlicher Aspekte, automatisierte Entscheidung, Profiling
- bei umfangreicher Verarbeitung sensitiver Daten
- bei systematischer umfangreicher Überwachung öffentlicher Räume
- bei Verarbeitungen gemäß Aufsichtsbehörden-Liste

Inhalt: Bewertung

- Beschreibung, Zweckerreichung, Risiken, Abhilfemaßnahmen, Einhaltung Verhaltensregeln

Verarbeitungsmanagement

Verarbeitungs-(fahrens-)verzeichnis (bisher §§ 4d, 4e, 4g Abs. 2 BDSG-alt, jetzt Art. 30 DSGVO)

Rechtmäßigkeitsprüfung (evtl. über Audit), evtl. Datenübermittlungskontrolle

Rollenkonzepte

Speicherfristenfestlegung und -verwaltung (Löschung/Sperrung bisher § 35 Abs. 2, 3 BDSG-alt, jetzt Art. 17, 18 DSGVO)

→ Differenzierung nach Art der Daten: Produktion, (Tele-) Kommunikation, Video/Kontrolle, Personal, Finanzen, AO/ HGB, Protokollierung

Auftragsmanagement

Cloud-Computing, Nutzung externer Software, Einsatz v. Dienstleistern

- Bisher § 11 BDSG/jetzt Art. 28, 29 DSGVO: Auftraggeber (AG) kontrolliert Auftragnehmer (AN)
- Realität: AN bestimmt DV beim AG
- Spezialproblem: Drittauslands-ADV

→ Ziel: digitale Souveränität von AG, Mitbestimmungsmöglichkeit d. BR

- Dokumentation der Auftragsbeziehungen (Aktualität!)
- TOM, u. a. Verschlüsselung und Pseudonymisierung, wo möglich
- Präzisierung der Weisungen gem. Betriebsvereinbarungen
- AN-Kontrolle (evtl. Einbezug von BR)

IT-Sicherheitsmanagement und Datenschutz

Technisch-organisatorische Maßnahmen (§ 9 BDSG-alt, Art. 32 DSGVO):

- Vertraulichkeit (z. B. Verschlüsselung)
- Integrität, Authentizität (z. B. elektronische Signatur)
- Verfügbarkeit (z. B. Backup, Stromversorgung)
- Intervenierbarkeit (Löschen, Sperren, Korrektur)
- Transparenz, Revisionsfähigkeit (Protokoll, Dokumentation)
- Nichtverkettbarkeit (z. B. Abschottung)

Evtl. kritische Infrastrukturen gem. BSI-Gesetz

→ Kooperation IT-Sicherheitsbeauftragter – bDSB – Betriebsrat

DSGVO-Instr.: Verhaltensregeln/ Zertifizierung

Verhaltensregeln → Art. 40, 41

EU oder national

Genehmigung und Registrierung

Überwachung durch akkreditierte Experten

Zertifizierung → Art. 42, 43

Förderung durch EU

Freiwillig und transparent (Kriterien, Notifikation, Registrierung)

Dauer max. 3 Jahre, Entzug durch Aufsicht od. Zertifizierungsstelle

Akkreditierung der Zertifizierungsstelle

EU-Kommission legt Standards fest

Betroffenenrechte - allgemein

Auskunft (incl. Akteneinsicht)

Sperrung, Löschung, Berichtigung

Widerspruch, Unterlassung, (Folgen-) Beseitigung

Geldentschädigung (Schadenersatz, Schmerzensgeld)

Anrufung DS-Behörde, Rechtsschutz

AN: Recht auf Lüge, evtl. Verwertungsverbot bei Kündigung

DSGVO-Instrumente: Betroffenenrechte

Transparenz

Grundsätze, Schutz der Betroffenenrechte → Art. 12

Informations- u. Benachrichtigungspflichten → Art. 13, 14

Auskunftsanspruch über Zweck, Datenkategorien, Empfänger, Speicherdauer, Betroffenenrechte, Herkunft, evtl. automatisierte Entscheidung, Auslandstransfer → Art. 15

Datenkorrektur

Berichtigung → Art. 16, Löschung → Art. 17, Sperrung/V.beschränkung → Art. 18

Sonstige

Portabilität → Art. 20, Widerspruch → Art. 21, Automatisierte Entscheidung → Art. 22, Beschwerde bei Datenschutzaufsicht → Art. 77, Schadenersatz → Art. 82

Einschränkungen → Art. 23: nationale Öffnungsklausel

DSGVO-Instrumente: Rechtsschutz

Rechtsschutzgarantie: Art. 47 EuGRCh

Klagebefugnis gg. Datenschutzaufsicht → Art. 78

Klagebefugnis gg. verarbeitende Stelle → Art. 79

Klagevollmacht f. Verband u. Verbandsklagemöglichkeit → Art. 80

UKlaG 2016, nicht Betroffenenvertretung und nicht im Beschäftigtendatenschutz

Aussetzung bei Parallelverfahren → Art. 81

Annullierung von EU-Entscheidungen durch EuGH → Art. 263 Vertrag über die Arbeitsweise der EU (AEUV); EuGH-Vorlageverfahren durch nat. Gerichte → Art. 267 AEUV (Bewährungsprobe Privacy Shield)

Keine Individualklage beim BVerfG, aber evtl. Verbandsklage über EuG

Sanktionen DSGVO

Rüge → Art. 58

Anordnung → Art. 58

Geldbußen bis max. 10 Mio. € od. 2% vom Umsatz bei weltweiten Unternehmen bei minderen u. formellen Verstößen, bis max. 20 Mio. € od. 4% bei grdl. materiellen Verstößen u. Missachtung von Anordnungen → Art. 83

Sonst national geregelte Sanktionen → Art. 84

Sonderregelungen

Freie Meinungsäußerung und Informationsfreiheit → 85

Öffentlicher Zugang zu amtlichen Dokumenten → 86

Nationale Identifikations-Kennziffer → 87

Beschäftigtendaten → 88

Archiv, Wissenschaft, Statistik, Geschichte → 89

Berufsgeheimnisse → 90

Kirchen und Religionsgemeinschaften → 91

→ Öffnungsklauseln

Links

- c't: Strengere Datenschutz-Vorschriften für Unternehmen und Konzerne
- Praxishilfen von der GDD zur Umsetzung der DSGVO, u.a. ein Mustervertrag zur Auftragsverarbeitung
- Durchsuchbare Liste der Privacy-Shield-zertifizierten US-Unternehmen
- Einführung in Schadenskategorien vom BSIEinführung in Schadenskategorien vom BSI
- BDSGaF
- DSGVO