GDPR/DSGVO – Was müssen Mittelständler wissen?

Dr. Thilo Weichert
Netzwerk Datenschutzexpertise

Glory Innovation Forum 2018

Dienstag 19.09.2018 – Heiligendamm/Bad Doberan

Inhalt

- Rahmenbedingungen
- Verfassungsrecht – bisheriges Recht
- Datenschutz-Grundverordnung
  - Grundprinzipien
  - Spezielle Regelungen
  - Garantien und Schutzmaßnahmen
  - Datenschutzmanagement
  - Verhaltensregeln / Zertifizierung
  - Betroffenenrechte
  - Kontrolle
- Hausaufgaben

Technisch-struktureller Rahmen

- Aktuelle Digitalisierungstrends:
  Social Communities
  Mobile Computing
  Cloud Computing
  Big Data Analytics – künstliche Intelligenz
- Zielsetzungen (Zwecke) sind vielfältig und kombiniert
- Weitere Trends: Virtual Reality, Robotik, Biotechnik, Cyborgs
- Handel: Online-Einkauf (Amazon), ePayment, CRM, Online-Werbung

Wirtschaft/Industrie 4.0

Personenbezogene Daten als Rohstoff/Öl/Zahlungsmittel des 21. Jahrhunderts

> BITKOM/Bundesregierung:

Primat der Wirtschaft,

- Zurückdrängung des Datenschutzes
- Datenreichtum statt Datensparsamkeit
- Multifunktionale Datennutzung statt Zweckbindung

> Konkurrenzfähigkeit gegenüber USA/Süd-Ost-Asien

Rolle Deutschlands bei DSGVO-Gesetzgebung

- Widerspruch: Pochen auf hohem deutschen Datenschutzstandard vs. Bremsen des Gesetzgebungsprozesses und rückschrittliche Änderungsvorschläge

Beispiele

- Januar 2012 forderte BMI Friedrich Selbstregulierung vor Verordnung
- BMI propagierte Abschaffung d. Gesetzesvorbehalts im Privatbereich
- Richtlinie statt Verordnung > Subsidiaritätsrüge
- Noch Ende 2015 Angriffe auf Zweckbindung und Datensparsamkeit (Stichwort Big Data) durch Kanzlerin Merkel und Vizekanzler Gabriel

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 Integrität 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. **Diskriminierungsverbote**,

Art. 27 ff. Solidarität/Arbeitnehmerrechte

Art. 38 **Verbraucherschutz**

Art. 44 Petitionsrecht, Art. 47 Rechtsschutz

Bisherige Regelungen

- Allgemeines Datenschutzrecht, v. a. BDSG, EG-DSRl.
- TelekommunikationsG (TKG), TelemedienG (TMG)
- Verbraucherschutz bis 2016 kein digitales Spezialrecht
- Arbeitnehmer-Regelungen: § 32 BDSG, SGB, ASiG …

> Vertrag, Einwilligung od. Gesetz:
> Verhältnismäßigkeitsgrundsatz

Datenschutz-Grundverordnung u. neues Datenschutzrecht

Europäische Datenschutz-Grundverordnung (DSGVO)

- 24.05.2016 Inkrafttreten
- 25.05.2018 Direkte Anwendbarkeit

Bundesdatenschutzgesetz-neu (BDSGnF)

- Verabschiedung Bundestag 27.04, Bundesrat 12.05.2017
- Inkrafttreten 25.05.2018

Privacy-Verordnung ersetzt künftig EU-TK-DSRiLi

- Verabschiedung Ende 2018, Anwendbarkeit Ende 2020 (?)
- Bis dahin weiterhin Gültigkeit von TKG und TMG (eingeschränkt)

7 Regeln des Datenschutzes

- Rechtmäßigkeit (Art. 5 ff. DSGVO)
- Einwilligung (Art. 7 DSGVO)
- Zweckbindung (Art. 5 I lit. b DSGVO)
- Erforderlichkeit und Datensparsamkeit (Art. 5 I lit. c, e DSGVO)
- Transparenz und Betroffenenrechte (Art. 12 ff. DSGVO)
- Datensicherheit (Art. 25, 32 DSGVO)
- Kontrolle (Art. 51 ff. DSGVO)

Inhalte der allgemeinen Datenschutznormen

- Interessenabwägung zwischen Verarbeiter und Betroffenen
- Mächtiger Vertragspartner definiert Geschäftsmodell
- Absolute Tabuzonen: Kernbereich persönliche Lebensgestaltung, vollständige Persönlichkeitsbilder
- Bes. Begründungspflicht und strenge Verhältnismäßigkeitsprüfung: bes. Datenarten, Berufsgeheimnisse, Einwilligung

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

Anwendungsbereich (2, 3)

Generelle Anwendbarkeit – Ausnahmen:

- Justiz und öffentliche Sicherheit > DSRl Polizei-Justiz (zeitgleich)
- Außenpolitik, Nationale Sicherheit (Geheimdienste)
- EU-Institutionen
- Persönliche und familiäre Zwecke
- Telekommunikation > künftig ePrivacy-Verordnung

Räumlich

- Marktort, EU-Einwohner als Betroffene

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. 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

Bundesdatenschutzgesetz – neu (BGBl. 2017 I S. 2097)

- Regelung der Videoüberwachung (4) str. ob Regelungsbefugnis im Privatbereich
- Beibehaltung der (betrieb-/behördlichen) DSB (5-7, 38)
- Verarbeitung besonderer Kategorien personenbezogener Daten (22)
- Regelung Beschäftigtenverhältnis (26) erweiterter 32 BDSG-alt
- Wissenschaftliche od. historische u. statistische Zwecke (27)
- Einschränkung der Informations- und Auskunftsansprüche der Betroffenen (32-34)
- Berufsgeheimnisse Einschränkung der Betroffenen- und Kontrollrechte (29) eindeutig verfassungswidrig
- Scoring/Bonitätsauskünfte (31) Automatisierte Verfahren Versicherungen (37)
- Aufsichtsbehörden der Länder (40)

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)

Streitig, ob anwendbar auf Online-Direktmarketing

(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 (Betriebsrat, Zertifizierung, Einschaltung DSB)

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

Datenschutzmanagement nach DSGVO

- Verantwortlichkeit Art. 5 II, 24, 31 (Rechenschaftspflicht, Sicherstellung, Nachweis, Überprüfung, Aktualisierung; Kooperation mit Aufsicht)
- Informationspflichten (Art. 12 ff.)
- 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

Verarbeitungsverzeichnis (Art. 30)

- Verantwortlicher
- Zwecke der Verarbeitung (Differenzieren: CRM, Produktion, (Tele-) Kommunikation, Video/Kontrolle, Personal, Finanzen, AO/HGB, Protokollierung)
- Beschreibung der Art der Daten und der Betroffenen
- Übermittlungsempfänger und Auftragsverarbeiter (einschließlich Drittländer)
- Löschungsfristen (wenn möglich)
- Technisch-organisatorische Maßnahmen (wenn möglich)

Abs. 5: Keine Pflicht zur Erstellung bei weniger als 250 Mitarbeiter, wohl aber bei besonderem Risiko, bei sensitiven Daten

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

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

- 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 sind zulässig (Art. 37 II, III)
- Freiwillig eigener od. Verbands-DSB (Art. 37 IV)

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

- Interne 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 Abberufungsmöglich-keit (§ 40 Abs. 5 S. 2 BDSG)

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)

a) Unterrichtung u. Beratung von Leitung u. Beschäftigten

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

c) Beratung u. Überwachung der Datenschutz-Folgenabschätzung

d) 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

Auftrags-Management

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 u. 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

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)

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

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 (AGB und materielles Recht)

- 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

Aufsichtsbehörden

- Unabhängigkeit > 51, 52, Angemessene Ausstattung > 52 IV
- Legitimation, Qualifikation > 53
- Zuständigkeit der Lead Authority bei Hauptniederlassung > 56
- Aufgaben: Kontrolle und Sanktion, Öffentlichkeitsarbeit, Beratung, Beschwerdebearbeitung, Kooperation, Genehmigungen u. Akkreditierungen > 57
- Befugnisse: Untersuchung, Sanktion (Rüge, Anordnung, Bußgeld), Information > 58

Bisher keine Transparenz bei Bestellung, begrenzte (nicht justiziable) Qualitätsanforderungen

Teils katastrophale Ausstattung

Kooperation und Kohärenz

- Zusammenarbeit zw. Lead-Authority und anderen Aufsichtsbehörden: Entwurfszusendung, Reaktionszeit 4 Wochen, Betroffeneninfo durch Beschwerdebehörde > 60, 61, Gemeinsame Maßnahmen mit Teilnahmerecht > 62
- Kohärenzverfahren über Europäischen Datenschutzausschuss bei gemeinsamem Interesse, Mehrheitsprinzip > 63, 64, Konfliktlösung in Einzelfällen mit 2/3-Mehrheit > 65

> Massiver Arbeits- und Aufgabenzuwachs

Europäischer Datenschutzausschuss (EDA)

- Eigene Rechtspersönlichkeit, 1 Vertretung pro Land, Teilnahmerecht der EU-Kommission > 68
- Unabhängigkeit > 69
- Aufgaben: Überwachen, Beraten, Untersuchen, Fördern, Stellungnehmen, Registerführen, Berichten > 70, 71

Unabhängige Länderrepräsentanz nicht gewährleistet > 17-19 BDSG-neu

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

Sonstige Sanktionen: Abmahnmöglichkeit (Umfang umstritten)

Sonderregelungen in DSGVO

- 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

Wichtige Veränderungen gegenüber bisherigem Datenschutzrecht in der DSGVO I

- Privilegierung der Weiterverarbeitung für Zwecke der Forschung, der Statistik und der Archive (Art. 5 I lit. b, 85, 89)
- Aufwertung der Datenminimierung (Art. 5 I lit. c, e)
- Koppelungsverbot (Art. 7 IV)
- Regelung zu Kindereinwilligung (Art. 8)
- Verbesserung der Transparenzregelungen (Art. 12-15)
- Portabilität – Datenübertragbarkeit (Art. 20)
- Regelung des „Profiling“ (Art. 4 Nr. 4, 22) incl. „automatisierte Entscheidungen“ (Generalregelung zu Big Data)

Wichtige Veränderungen gegenüber bisherigem Datenschutzrecht in der DSGVO II

- Privacy by Design/Privacy by Default (Art. 25)
- Schutzzielbestimmungen (Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit) für technisch-organisatorische Maßnahmen incl. Pseudonymisierung/Verschlüsselung, Backup, Monitoring (Art. 32)
- Risikobasierter Ansatz mit Datenschutz-Folgenabschätzung (Art. 35) u. vorheriger Konsultationspflicht (Art. 36)
- Europaweite Etablierung des Datenschutzbeauftragten (Art. 37 ff.)
- Aufwertung der Verhaltensregeln (Art. 40 f.)
- Einführung formeller Datenschutzzertifizierungen (Art. 42 f.)

Wichtige Veränderungen gegenüber bisherigem Datenschutzrecht in der DSGVO III

- Ausdifferenziertere Regelungen zur Drittlandsübermittlung (Art. 44 ff.) incl. Angemessenheitsbeschluss, Standardvertragsklauseln, Binding Corporate Rules, unter Berücksichtigung des EuGH-Beschlusses zu Safe Harbor (dennoch jetzt Privacy Shield)
- Einheitliche Regelungen zur Datenschutzaufsicht (Art. 50 ff.) mit erheblich erweiterten Aufgaben
- Komplexe Regelung von Zusammenarbeit und Kohärenz (Art. 60 ff.) mit qualifizierten Mehrheitsbeschlüssen des Europäischen Datenschutzausschusses (EDSA, Art. 68 ff.)
- Verbesserte Rechtsschutz- und Sanktionsmöglichkeiten

Hausaufgaben

Unternehmen

- Etablierung eines DSGVO-konformen Datenschutzmanagements
- Evtl. Durchführung der Datenschutz-Folgenabschätzungen
- Vereinbarung bei gemeinsamer Verantwortung (Art. 26 DSGVO)
- Anpassung der Auslandsdatenübermittlungen
- Abschluss Kollektiv-/Betriebsvereinbarungen
- Etablierung von Zertifizierungsverfahren

Unternehmensverbände/Beschäftigtenvertretungen

- Erarbeitung von Verhaltensregeln/Kollektivvereinbarungen

GDPR/DSGVO – Was müssen Mittelständler wissen?

Thilo Weichert
Waisenhofstr. 41, 24103 Kiel
0431 9719742
weichert@netzwerk-datenschutzexpertise.de
www.netzwerk-datenschutzexpertise.de