FIDES IT Consultants

Die EU-Datenschutz-Grundverordnung und das Bundesdatenschutzgesetz (neu)

Osnabrück, den 15.08.2017

Bremen, den 17.08.2017

Hamburg, den 07.09.2017

Dr. Ralf Kollmann

FIDES IT Consultants

Agenda

DSGVO und BDSG neu

1. Überblick DSGVO und BDSG neu
2. Aufbau des Datenschutzmanagements

Auftragsverarbeitung

1. Auftragsverarbeitung nach altem und neuem Recht
2. Konzerndatenverarbeitung

Direktwerbung

1. Postalische Werbung
2. Elektronische Werbung

FIDES IT Consultants

Übersicht der Datenschutz-Rechtslage

DSGVO (ab 25. Mai 2018)

- Die DSGVO gilt unmittelbar in jedem Mitgliedsstaat von Europa, ohne dass sie in nationales Recht umgewandelt werden muss.
- Öffnungsklauseln bieten nationalen Gesetzgebern die Möglichkeit eigener Regelungen.

BDSG neu (ab 25. Mai 2018)

Ausfüllung der Öffnungsklauseln der DSGVO

Spezialgesetze mit Datenschutzbezug, bspw.:

- TMG, TKG gelten bereits und haben größtenteils weiterhin Gültigkeit
- Sozialgesetzbücher gelten bereits und haben weiterhin Gültigkeit
- **EU-Privacy-Verordnung (Entwurf, geplant ab 25. Mai 2018)**
  Ersetzt einzelne Regelungen aus TMG, TKG und UWG

Grundsätze der Verarbeitung

Grundlegende Paradigmen des BDSG gelten zukünftig auch auf Grundlage der DSGVO, bspw.:

- Verbot mit **Erlaubnisvorbehalt** (Art. 6)
- **Transparenz** (Art. 5 Abs. 1 lit. a, EG 39)
- **Zweckbindung** (Art. 5 Abs. 1 lit. b, EG 39)
- **Datensparsamkeit** (Art. 5 Abs. 1 lit. c, Art. 25 Abs. 2, EG 39, EG 78)
- Technische und organisatorische **Schutzmaßnahmen** (Art. 25, Art. 32)

Neue Grundsätze der DSGVO, insbesondere:

- "**Treu und Glauben**" (Art. 5 Abs. 1, EG 39, 45)
- **Nachweisbarkeit** (diverse, u.a. Art. 5 Abs. 2, Art. 24, EG 39, EG 78)
- **Risikobewertungen** nach Eintrittswahrscheinlichkeit und Schadenshöhe (u.a. Art. 24, 25, 32, EG 76-78)

Rechtsgrundlagen 1

- **Einwilligung** (Art. 6 Abs. 1 lit. a, Art. 7, EG 42)
  - Sonderregelung zur Einwilligung für / durch **Kinder** (Art. 8)
- Erfüllung eines **Vertrags** (Art. 6 Abs. 1 lit. b)
- Erfüllung einer **rechtlichen Verpflichtung** (Art. 6 Abs. 1 lit. c)
- Wahrung **berechtigter Interessen** (Art. 6 Abs. 1 lit. f, EG 47, 48)
  - Interessenabwägung erforderlich
  - Kinder gesondert zu berücksichtigen

Rechtsgrundlagen 2

- **Zweckänderung** (Art. 6 Abs. 4, 13 Abs. 3, EG 50, §§ 24, 32 BDSG neu)
  - **Prüfung der Vereinbarkeit** erforderlich
  - Regelmäßig vereinbar:
    - Wissenschaftliche Forschungszwecke (EG 50)
    - **Statistische Zwecke** (EG 50)
  - Bei positivem Ergebnis gilt die Rechtsgrundlage der ursprünglichen Verarbeitung
  - **Informationspflicht** über die Zweckänderung (Art. 13 Abs. 3)
  - **Ausnahme** von dieser Informationspflicht ggf. bei **analoger Verarbeitung** (§ 32 Abs. 1 Nr. 1BDSG neu)
  - **Neu:** Erweiterte Zulässigkeit der Zweckänderung bei Geltendmachung, Ausübung oder Verteidigung **zivilrechtlicher Ansprüche** (§ 24 Abs. 1 Nr. 2 BDSG neu)

- Aufgabe **öffentlichen Interesses / öffentlicher Gewalt** (Art. 6 Abs. 1 lit. e, § 3 BDSG neu)

Rechtsgrundlagen 3

- **Schutz lebenswichtiger Interessen** (Art. 6 Abs. 1 lit. d)

- **Besondere Daten** (Verbot mit Erlaubnisvorbehalt, Art. 9)
- Zulässigkeitserweiterung für **Gesundheitsdaten** (§ 22 BDSG neu)
  - Gesundheitsvorsorge und Medizinische Diagnostik
  - "Verwaltung von Systemen und Diensten" im Gesundheits- und Sozialbereich
  - **Beurteilung der Arbeitsfähigkeit eines Beschäftigten**
  - Verträge mit Angehörigen eines Gesundheitsberufs
  - **Verarbeitung durch Ärzte** oder **andere der Geheimhaltungspflicht Unterliegende**
  - Aus Gründen des öffentlichen Interesses im **Bereich der öffentlichen Gesundheit**

- Zusätzliche **spezifische technische und organisatorische Schutzmaßnahmen** sind zu treffen.

Betrieblicher Datenschutzbeauftragter 1

Bestellung zum Datenschutzbeauftragten gemäß DSGVO (Art. 37, 38)

- Verarbeitung durch **Behörden**
- **Kerntätigkeit** des Verantwortlichen oder Dienstleisters …
  - … erfordert eine umfangreiche, regelmäßige und **systematische Überwachung** von betroffenen Personen
  - … besteht in der umfangreichen **Verarbeitung besonderer Daten** (Art. 9) oder **Daten über strafrechtliche Verurteilungen** und Straftaten (Art. 10)

Betrieblicher Datenschutzbeauftragter 2

Bestellung gemäß BDSG neu (§ 38 BDSG neu):

1. Verantwortlicher oder Dienstleister führen Verarbeitungen durch, die einer **Datenschutz-Folgenabschätzung** unterliegen
2. Verarbeitung personenbezogener Daten geschäftsmäßig
   - zum Zweck der **Übermittlung**
   - zur anonymisierten Übermittlung
   - zur Übermittlung für Zwecke der **Markt- oder Meinungsforschung**
3. Mindestens **zehn Mitarbeiter** verarbeiten personenbezogene Daten automatisiert

Im Ergebnis sind die Vorschriften zur Bestellung weitreichender als im BDSG a.F.

FIDES IT Consultants

Rechte der Betroffenen 1

- Transparente Information, Kommunikation und Modalitäten (Art. 12)
- Informationspflicht bei **Direkterhebung** (Art. 13, §§ 29, 32 BDSG neu)
- Informationspflicht bei **indirekter Erhebung** (Art. 14, §§ 29, 33 BDSG neu)
- **Auskunftsrecht** (Art. 15, §§ 29, 30, 34 BDSG neu)
- Recht auf **Berichtigung** (Art. 16)
- Recht auf **Löschung** ("Vergessenwerden", Art. 17, § 35 BDSG neu)
- **Einschränkung** der Verarbeitung ("Sperrung", Art. 18 , § 35 BDSG neu)
- **Mitteilungspflicht** (Weiterleitung / Kaskade, Art. 19)
- Recht auf **Datenübertragbarkeit** ("Datenmobilität", Art. 20)
- **Widerspruchsrecht** (Art. 21, § 36 BDSG neu)
- **Automatisierte Entscheidungen** / Profiling (Art. 22, §§ 31, 37 BDSG neu)
- **Datenpannen** (Art. 33, 34, § 29 BDSG neu)

SONDERREGEL: VERBRAUCHERKREDITE

SONDERREGEL: VERSICHERUNGEN

Rechte der Betroffenen 2

Fazit

Die Rechte der Betroffenen haben in der DSGVO einen hohen Stellenwert (breite, zentrale Aufstellung, Bußgelder).

Die Beurteilung und Umsetzung wird durch zahlreiche Sonderregelungen des BDSG neu komplexer.

Stellenweise bestehen Sonderregelungen für Branchen und spezielle Verarbeitungsfälle (bspw. Versicherungen, Gesundheitswesen, analoge Verarbeitung).

Datenschutz-Folgeabschätzungen 1

Datenschutz-Folgeabschätzungen (DSF) dienen als Nachfolgeregelung zur Vorabkontrolle.

Verpflichtung zur Durchführung bei (Art. 35 Abs. 3)

- Systematischer / umfassender **Bewertung persönlicher Aspekte**, inkl. **Profiling**
- **Verarbeitung besonderer Daten** (Art. 9 Abs. 1) bzw. Straftaten (Art. 10)
- Systematischer **Überwachung** öffentlich zugängiger Bereiche (Videoüberwachung)

- **Konsultation der Aufsichtsbehörde**, wenn ohne getroffene Maßnahmen ein hohes Risiko bestünde (Art. 36)

Datenschutz-Folgeabschätzungen 2

Hinweise auf Erfordernis zur Durchführung:

- "**Innovative Technologien**" / Technologiewechsel (insb. ohne bisherige DSF)
- **Neue IT-gestützte Geschäftsprozesse** (insb. ohne bisherige DSF)
- **Große Menge** personenbezogener Daten bzw. große Zahl Betroffener
- Verarbeitung **besonders sensibler Daten** (bspw. Gesundheitsdaten, biometrische Daten, Leistungsdaten, Finanzdaten)
- **Verarbeitung mit Rechtswirkung** gegenüber natürlichen Personen

Datenschutz-Folgeabschätzungen 3

Zusammenfassung des Prozesses

1. Prüfung auf Erfordernis
2. Durchführung
3. Konzeption zu treffender Schutzmaßnahmen
4. Zyklische Folgeprüfungen auf Einhaltung und Wirksamkeit
5. Ggf. Veranlassung und Kontrolle von Anpassungsmaßnahmen

Dokumentation

Wer führt die DSF durch?

- **Formal zuständig** und verantwortlich für die Durchführung ist der "Verantwortliche", d.h. das Unternehmen (Art. 25 Abs. 1 und EG 84).
- **Faktisch** wird die Veranlassung und Umsetzung regelmäßig in den Händen des bDSB liegen, wobei durch ihn erforderliche Mitarbeiter / Dritte hinzugezogen werden sollten.

Schutzverletzungen (Datenpannen) 1

Definition einer "Verletzung des Schutzes" (Art. 4 Abs. 12)

- **Vernichtung**, **Verlust** oder **Veränderung** von personenbezogenen Daten
- **Unbefugte Offenlegung** oder **unbefugter Zugang** [zu personenbezogenen Daten]
- Personenbezogene Daten wurden übermittelt, gespeichert oder auf sonstige Weise verarbeitet

Schutzverletzungen (Datenpannen) 2

Voraussetzung für das Eintreten

- Rechtzeitige bzw. **angemessene Reaktion** [auf ein die Datenverarbeitung i.w.S. betreffendes Ereignis] **ist unterblieben**
- **Mögliche Auswirkungen** (entscheidend ist das Potential) beinhalten:
  - Physische,
  - materielle oder
  - immaterielle

  Schäden für natürliche Personen

Schutzverletzungen (Datenpannen) 3

Mögliche Auslöser einer Schutzverletzung

- Datenverlust
  - Fehlende oder fehlerhafte Datensicherung (Backup)
  - Verlust von Mobilgeräten und Datenmedien
- "Hackerangriff" i.V.m. Datendiebstahl oder Datenmanipulation
- Ungenügender Zutritts- bzw. Zugangsschutz
- Fehlerhafte Berechtigungseinstellungen
- Fehlgeleitete E-Mail

Zentrales Kriterium: Ein Risiko für die Rechte und Freiheiten von Personen besteht.

Dies gilt es, bei der Risikobeurteilung belastbar einzuordnen und bei Nichtvorliegen nachvollziehbar zu begründen.

Schutzverletzungen (Datenpannen)

Schutzverletzungen und Auswirkungen

in Ihrem Unternehmen ?

Schutzverletzungen (Datenpannen) 4

Beispiele für Schutzverletzungen und Auswirkungen (EG 85)

- "**Verlust der Kontrolle**" über personenbezogenen Daten
- **Einschränkung der Rechte** einer natürlichen Person
- Diskriminierung
- Identitätsdiebstahl oder -betrug
- Finanzielle Verluste
- Rufschädigung
- **Unbefugte Aufhebung einer Pseudonymisierung**
- **Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten**
- Andere erhebliche **wirtschaftliche oder gesellschaftliche Nachteile**

Agenda

Aufbau des Datenschutzmanagements

Ermittlung des Handlungsbedarfs 1

Zentrale Fragen

- In welchen **Geschäftsprozessen** werden personenbezogene Daten verarbeitet?
- Um welche **Art von Daten** handelt es sich?
- **Wer** ist betroffen?
- **Wo** werden die Daten verarbeitet (welche Systeme? Ausland?)
- Welche **normativen Vorgaben** zur Verarbeitung bestehen?
- Wie sind die **Daten geschützt?** Ist der **Schutz angemessen?**

Ermittlung des Handlungsbedarfs 2

Durchführung einer Prozess- und Systemaufnahme

Welche Maßnahmen wurden bereits getroffen? Sind Anpassungen erforderlich?

- **Geschäftsprozesse**
  - Operative Prozesse
  - Verwaltung
  - Werbung
  - Arbeitnehmerdatenschutz
  - Standorte
  - …
- **IT-Systeme / Verfahren**
  - Server, Datenbanken, Clients, …
  - Automatisierte Verarbeitung
  - Profiling
  - Massenverarbeitung
  - Data Warehouse / Big Data
  - …
- **Daten**
  - Stammdaten, Kontaktdaten
  - Bewegungsdaten
  - Aggregierte Daten / Statistik / Controlling
  - Besondere Daten
  - Werbung
  - …
- **Datenschutz-Prozesse**
  - Rechtsgrundlagen
  - Auftragsverarbeitung
  - Datenschutz-Folgenabschätzungen
  - IT-Sicherheit / TOM
  - Datenschutz-Management
  - …

Ermittlung des Handlungsbedarfs 3

Durchführung einer GAP-Analyse, insbesondere:

- **Datenschutz- und IT-Sicherheitsmanagement** (Status Quo, Dokumente)
- **Rechtsgrundlagen** der Datenverarbeitung
  (Ermittlung, Prüfung bzw. Sicherstellung erfolgt? Insbesondere bei Prozessen mit starkem IT-Bezug (Data Mining, Profiling, Scoring, Video, ggf. Werbung)
- **Nachweispflichten** (Identifikation von Dokumentationslücken und Anforderungen)
- **Informationspflichten** (Ermittlung und Sicherstellung der Erfüllung)
- **Betroffenenrechte** (systematische Einhaltung)
- **Auftragsverarbeitung**
  - **Inventarisierung** und Prüfung von ADV-Verträgen und Funktionsübertragungen
  - Technische und organisatorische **Schutzmaßnahmen**
  - **Konzerndatenverarbeitung**
  - **Bei Dienstleistern:** Identifikation und Adressierung **neuer Haftungsrisiken**
- **Werbemaßnahmen** (Inventarisierung, datenschutzkonforme Gestaltung)

Datenschutzorganisation – Aufbau Datenschutzkonzept 1

Konzeption des Datenschutzmanagements

Die Ergebnisse der GAP-Analyse führen zur Konzeption des Datenschutzmanagements und Dokumentation im Datenschutzkonzept.

Ziele eines Datenschutzkonzepts

- Sicherstellung der **Rechtmäßigkeit** der Datenverarbeitung
- **Nachweis** einer angemessenen Datenschutzorganisation

- Aber in erster Linie: **Arbeitshandbuch**
  - **Status Quo** des Datenschutz-Managements
  - **Organisation** von Datenschutz-Prozessen
  - **Unterstützung** des IT-Projektmanagements

Datenschutzorganisation – Aufbau Datenschutzkonzept 2

Inhalte des Datenschutzkonzepts

Beschreibung von Datenschutzprozessen, Prüfungen, bspw. jährliche Revisionszyklen, DSF, ADV, Aufgaben, Dokumentenübersicht, insbesondere:

- Datenschutzrichtlinie
- IT-Sicherheitsrichtlinie
- Verzeichnis der Verarbeitungstätigkeiten
- Datenschutz-Schulungskonzept
- Dokumentation von Rechtsgrundlagen
- Verzeichnis der Datenschutzprozesse (Organisation des Datenschutzmanagements)
- Mitarbeitervereinbarungen (bspw. dienstliche und private Nutzung der IT, BYOD, Regelungen für Abwesenheit und Vertretung, Vertraulichkeit, Betriebs- und Geschäftsgeheimnisse, Vorgehen bei Datenpannen, Einwilligungen bei besonderen Verfahren bzw. zur Biometrie etc.)

Datenschutzorganisation – Aufbau Datenschutzkonzept 3

Beispiele für Datenschutz-Prozesse

- **Bestellung** des betrieblichen Datenschutzbeauftragten
- Aufnahme / Update der Verfahren für das Verzeichnis der **Verarbeitungstätigkeiten** (Art. 30 Abs. 1)
- Aufnahme / Anpassung / Update der **technischen und organisatorischen Schutzmaßnahmen** (TOM)
- **Auftragsverarbeitung** (Inventarisierung, Abschluss, Prüfung)
  - **AV-Dienstleister**: Zusätzliches Verzeichnis nach Art. 30. Abs. 2
- **Datenschutz-Folgeabschätzungen**
- Prüfung von **Rechtsgrundlagen** (bspw. Werbung, Arbeitnehmerdaten, Video)
- **Schutzverletzungen ("Datenpannen")**
- Maßnahmen zur **Wahrung der Betroffenenrechte** bspw.
  - Informations- und Auskunftsverfahren
  - Widerspruchsmanagement
  - Löschung, Berichtigung und Sperrung

Ihr Rechner ist gesperrt.

Alle Dateien auf dem Rechner wurden mit AES-128 verschlüsselt.

Die Entschlüsselung ist nur mit einem privaten Schlüssel möglich, der sich auf unserem Server befindet.

Um die Dateien wiederherzustellen, zahlen Sie 2 Bitcoins.

Folgen Sie dazu folgendem Link:

https://asgdf96g8df6s8s7df6sdf.onion/29834723423

IT-Sicherheit hilft

IT-Sicherheitsmanagement – Schutzziele und Kontrollen 1

Durch die DSGVO wird der Aufbau eines systematischen IT-Sicherheitsmanagements explizit gefordert.

Schutzziele / Anforderungen an die Maßnahmen

- Vertraulichkeit (bspw. durch Berechtigungen, Pseudonymisierung, Verschlüsselung)
- Integrität
- **Verfügbarkeit**
- Belastbarkeit
- Wiederherstellbarkeit von Daten bzw. Zugang zu selbigen

IT-Sicherheitsmanagement – Schutzziele und Kontrollen 2

Anforderungen an die Überwachung der Maßnahmen

- Einrichtung eines **Kontrollverfahrens**
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der **Wirksamkeit** der getroffenen Schutzmaßnahmen
- Gewährleistung der **Sicherheit der Verarbeitung**

IT-Sicherheitsmanagement – Konzeptionelle Anforderungen der DSGVO

Anforderungen an die Konzeption zu treffender Maßnahmen

Berücksichtigung von:

- **Stand der Technik** (→ ggf. Anpassung erforderlich, auch wenn die Verfahren unverändert bleiben)
- Implementierungskosten
- Art und Umfang der Datenverarbeitung
- Verarbeitungszwecken
- **Risikobeurteilung** nach Eintrittswahrscheinlichkeit und Schadenshöhe
- **Nachweisbarkeit**

Noch Fragen?

FIDES IT Consultants

In eigener Sache - Seminarankündigung

"Aufbau eines Datenschutzmanagements nach BDSG neu und Datenschutz-Grundverordnung"

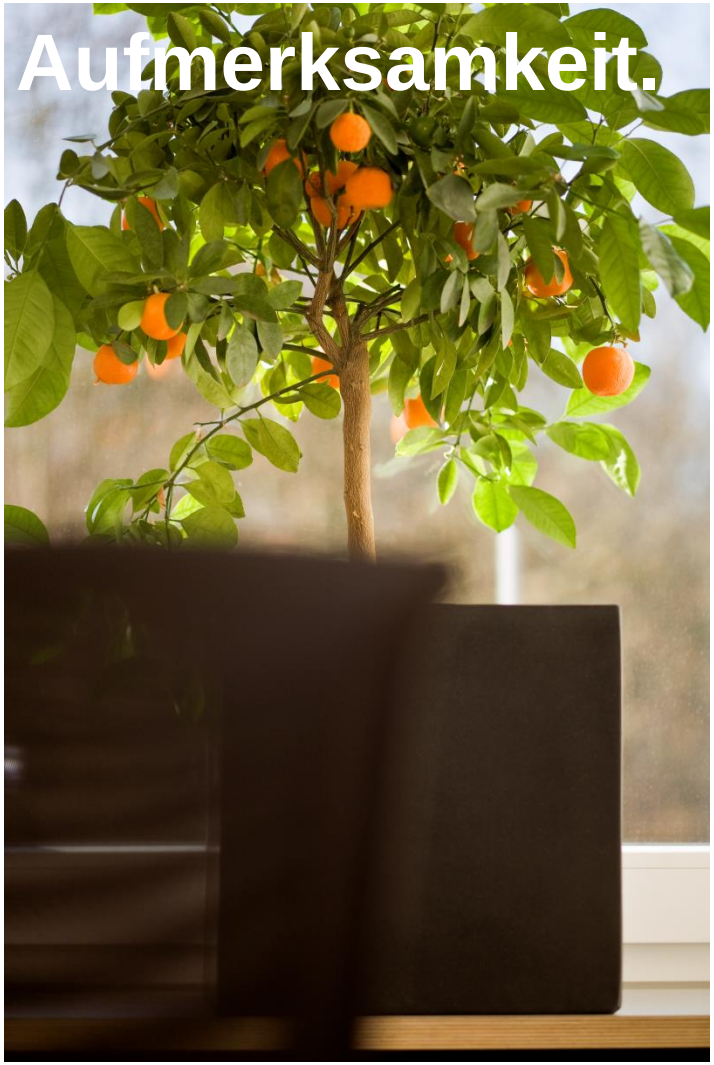
Themen

- Pflichten des betrieblichen Datenschutzbeauftragten
- Dokumentations- und Nachweispflichten
- Auftragsdatenverarbeitung
- Werbung
- Arbeitnehmerdatenschutz
- Technische und organisatorische Schutzmaßnahmen zum Datenschutz
- Anforderungen an ein IT-Sicherheitsmanagement

Datum: 26. Oktober 2017

Ort: Seminarräume der FIDES in der Niederlassung Bremen, Birkenstraße 37

Vielen Dank für Ihre Aufmerksamkeit.



Dr. Ralf Kollmann
r.kollmann@fides-it-consultants.de
T +49 421 3013 408
M +49 174 9280 408
F +49 421 3013 449

FIDES IT Consultants GmbH
Birkenstraße 37
28195 Bremen
Am Kaiserkai 60
20457 Hamburg

www.fides-it-consultants.de