ALPMANN FRÖHLICH.

Gemeinsam. Stark.

FORUM!-Wirtschaftsfrühstück

Stroetmanns Fabrik 06.02.2018

EU-Datenschutzgrundverordnung (DSGVO) - Was muss mein Unternehmen (in der Praxis) wissen?

- Hinweis:

  Die nachfolgenden Folien geben lediglich einen kurzen und unvollständigen Überblick über einige Neuerungen im Datenschutzrecht. Wir haften nicht für die Richtigkeit und Rechtmäßigkeit des Inhalts.

I. Historie

- Vorgeschichte: Unterschiedliche Datenschutzmodelle innerhalb der EU
- 2012 bis 2015: Gesetzgebungsverfahren
- 04.05.2016: Veröffentlichung im EU-Amtsblatt
- 24.05.2016: Inkrafttreten
- 25.05.2018: Geltung unmittelbar in allen Mitgliedstaaten
- 25.05.2018: Geltung des BDSG (neu); vollständiger Ersatz des BDSG (alt)
- 30.03.2019: GB wird „Drittland“ iSd DSGVO (Mitteilung der Kommission vom 09.01.2018)

II. Grundprinzipien des BDSG / DSGVO

- Sachlicher Anwendungsbereich (Art. 2): Verarbeitung personenbezogener Daten
- Personenbezogene Daten (Art. 4): alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen
- Räumlicher Anwendungsbereich (Art. 3): Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.

- Grundsätze für die Verarbeitung (Art. 5 DSGVO)
  - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht
- Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO)

  „die Verarbeitung ist nur zulässig, wenn …“
- Wichtige Erlaubnistatbestände:
  - Art. 6 Abs. 1, lit. a): Einwilligung
  - Art. 6 Abs. 1, lit. b): Erfüllung eines Vertrages
  - Art. 6 Abs. 1, lit. f): zur Wahrung berechtigter Interessen erforderlich, sofern nicht die Interessen der betroffenen Person überwiegen; Konzernprivileg? Direktmarketing?

- Privacy by design (Art. 25 Abs. 1)

  Datenschutz durch Technikgestaltung: der Schutz personenbezogener Daten erfolgt durch Ergreifung technischer und organisatorischer Maßnahmen (TOM); z.B. Pseudonymisierung und Anonymisierung

- Privacy by default (Art. 25 Abs. 2)

  Datenschutz durch datenschutzfreundliche Voreinstellungen: Werkeinstellungen sind datenschutzfreundlich auszugestalten

III. Haftung und Recht auf Schadenersatz

Art. 82 Abs. 1 DSGVO:
Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

1. Verstoß gegen die Verordnung:
- Dokumentations- und Nachweispflichten
- Lösch- und Berichtigungspflichten
- Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen
- Datensicherheit
- Informationspflichten

2. Anspruchsberechtigt:

- Jede Person, der wegen eines Datenschutzverstoßes ein Schaden entsteht

3. Anspruchsverpflichtet:

- Unternehmen, das Zweck und Mittel der Datenverarbeitung festlegt.
- Ggfs. Haftung des Unternehmens für Auftragsverarbeiter

4. Schaden:

a) Vermögensschaden

b) immaterielle Schäden (z. B. Diskriminierung)

c) Schadenshöhe:

- Keine Tabellen
- Bisher überschaubar bei Datenschutzverstößen (§ 823 BGB)
- Erwartung: Anstieg

d) Beweislast:

- Verantwortlichen trifft Nachweispflicht (ggf. Beweislastumkehr)
- Haftung für jeden Mitarbeiter

e) Verbandsklagen:

- Nur Unterlassung / kein Schadensersatz
- Professionelle Kläger / Prozessfinanzierer

Bußgelder nach DSGVO

1. Bisher: bis zu 300.000,- EUR (§ 43 Abs. 3 S. 1 BDSG)

2. Art. 83 Abs. 4 DSGVO:

- Empfindliche Bußgelder für fast jeden Verstoß gegen Vorschriften der DSGVO, die an Verantwortliche bzw. Auftraggeber gerichtet sind
- Behörde hat Ermessen; weiter Ermessensspielraum von Verwarnung bis zu Bußgeld in Höhe von 20 Mio EUR bzw. 4 % des weltweiten Jahresumsatzes
- Grundsatz: Verhältnismäßigkeit/ Abschreckung
- Kriterien: u. a. Dauer der Verstöße, Anzahl der Betroffenen, Schadenshöhe, Verschulden, Erstverschulden

- Beispiele (nicht abschließend) für Verstöße mit Bußgeld bis zu 10 Mio. EUR/2 % des Jahresumsatzes:
  - Verstoß gegen Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
  - Verstoß gegen Meldepflicht gegenüber Datenschutzaufsicht
  - Verstoß gegen Meldepflicht gegenüber betroffenen Personen
  - Keine oder unzureichende Datenschutz-Folgenabschätzung
  - Keine oder unzureichende Bestellung eines Datenschutzbeauftragten

- Beispiele (nicht abschließend) für Verstöße mit Bußgeld bis zu 20 Mio. EUR / 4% des Jahresumsatzes:
  - Unzulässige Verarbeitung personenbezogener Daten
  - Verstoß gegen allgemeine Informationspflichten gegenüber betroffenen Personen
  - Verstoß gegen Auskunftsrecht der betroffenen Personen
  - Verstoß gegen Pflicht zur Datenlöschung
  - Verstoß gegen Widerspruchsrecht
  - Unzulässige Übermittlung personenbezogener Daten in ein Drittland

3. Handlungsempfehlung:

Einrichtung eines wirksamen Datenschutz Compliance Systems

IV. Bestellung eines Datenschutzbeauftragten

- Art. 37 Abs. 4 iVm. § 38 BDSG (neu)

  Datenschutzbeauftragter ist zu benennen, soweit der Verantwortliche oder Auftragsverarbeiter in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt
- Aufgaben (Art. 39) Aufgabenkreis ist erweitert worden:
  - Unterrichtung u. Beratung zu den Pflichten
  - Überwachung
  - Beratung im Zusammenhang mit der Datenschutzfolgenabschätzung
  - Zusammenarbeit mit der Aufsichtsbehörde
  - Anlaufstelle für die Aufsichtsbehörde
- Intern oder extern?

V. Sicherstellung Betroffenenrechte:

1.
Stärkung der Betroffenenrechte
Verletzungen bußgeldbewehrt

2.
Betroffenenrechte:

- Auskunft
- Berichtigung
- Löschung
- Einschränkung der Bearbeitung (bisher: Sperrung)
- Vergessenwerden
- Datenübertragbarkeit

a)
Auskunftspflichten :

Art. 15 Abs. 1 DSGVO:

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

a) die Verarbeitungszwecke;
b) die Kategorien personenbezogener Daten, die verarbeitet werden;
c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

b)

Recht auf Löschung:

- Daten müssen für den gewöhnlichen Gebrauch (z.B. Abruf über eine Kundendatenbank, Online-Abruf) unbenutzbar gemacht werden
- Löschung auf allen Datenträgen und Löschung sämtlicher Sicherheitskopien ist wohl nicht erforderlich

c)

Recht auf Datenübertragbarkeit:

- Daten müssen vom Betroffenen stammen
- Verarbeitung muss auf Grundlage einer Einwilligung des Betroffenen oder zur Erfüllung eines Vertrages mit dem Betroffenen erfolgen
- Herausgabe aller Daten, die sich auf den Betroffenen beziehen in strukturierter Form; gängiges maschinenlesbares Format
- Herausgabe an den Betroffenen

- Kein Recht auf Portabilität, wenn dadurch Rechte und Freiheiten Dritter beeinträchtigt würden (z.B. Urheberrechte, Betriebs- und Geschäftsgeheimnisse)

d)

Belehrungspflicht des Verantwortlichen im Rahmen allgemeiner Informationspflicht

e)

Frist:

Pflicht des Verantwortlichen, unverzüglich tätig zu werden, spätestens innerhalb eines Monats

f)

Rechtsbehelfsbelehrungspflicht, wenn Antrag des Betroffenen abgelehnt wird

g)

Was ist zu tun?

- Im Vorfeld Verfahrensweisen festlegen, wie Betroffenrechte erfüllt werden

VI. Verarbeitungsverzeichnis:

1.

Art. 30 DSGVO:

Führen eines Verzeichnisses aller Verarbeitungstätigkeiten:

- Name und Kontaktdaten des Verantwortlichen + etwaigen Datenschutzbeauftragten
- Zweck der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorie betroffener Daten
- Übermittlung von personenbezogenen Daten an Drittland oder an internationale Organisation
- Wenn möglich, Fristen für die Löschung der Datenkategorien
- Wenn möglich, Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1

2.

Aufsichtsbehörde muss Verfahrensverzeichnis auf Anfrage zur Verfügung gestellt werden.

- Nur Pflichtangaben offenlegen

VII. Folgenabschätzung:

Art. 35 DSGVO

- Bewertung von Risiken von Datenverarbeitungsvorgängen für den Datenschutz von Betroffenen im Vorfeld
- Betroffene sollen sich Art, Umfang, Umstände, Zweck der beabsichtigten Verarbeitung von personenbezogenen Daten vergegenwärtigen
- Geht um Verwendung maßgeblicher Systeme und Verfahren zur Bearbeitung
- Bußgeldbewehrt. Vor Einführung eines neuen Verfahrens: Folgenabschätzung vornehmen

VIII. Einwilligungsmanagement

- Prüfung, auf welcher Grundlage und zu welchem Zweck Daten verarbeitet werden
- Bisher erteilte Einwilligungen sollen fortwirken, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen
- Überprüfung Einwilligungserklärung (Art. 7):
  - Die Einwilligung muss im Hinblick auf einen bestimmten Verwendungszweck erteilt werden
  - Das Ersuchen um Einwilligung muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen
  - Die Einwilligungserklärung ist von anderen Erklärungen und/oder Sachverhalten klar zu trennen
  - Die Einwilligung kann jederzeit widerrufen werden
  - Die Einwilligung muss ohne Zwang erteilt werden

IX. Überprüfung Auftragsverarbeitung (Art. 28, 29 DSGVO)

- Auslagerung der Datenverarbeitung
- Art. 4 Nr. 8: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet
- Vertrag mit umfassenden Regelungen zur Art und Weise der Datenverarbeitung: Bestehende Verträge an DSGVO anpassen!
- Privilegierung fällt weg – Auftragsverarbeiter ist Dritter
- Unterscheidung zur Funktionsübertragung ist (wohl) obsolet
- Gesteigerte Pflichten des Auftragsverarbeiters und Mitverantwortung

Datentransfer ins Ausland (Art. 44 ff.)

- Angemessenes Schutzniveau? Beispiel USA: Von safe harbor zum privacy shield
- Wenn (-), Einwilligung, zur Erfüllung eines Vertrages erforderlich, Verwendung der Standardvertragsklauseln, konzernintern: genehmigte binding corporate rules
- neu: Anerkennung von Zertifikaten

X. DSGVO und Arbeitsrecht:

- Dargestellte Rechte und Pflichten gelten auch im Arbeitsverhältnis
- Besondere Regelungen in Art. 88 DSGVO und § 26 BDSG (neu)
- Problem: Freiwilligkeit der Einwilligung im Arbeitsrecht (vgl. § 26 Abs. 2 BDSG (neu))
- Daher Allgemeiner Erlaubnistatbestand in § 26 Abs. 1 BDSG (neu): Verarbeitung ist erlaubt, wenn es für die Begründung, Durchführung oder Beendigung erforderlich ist.

- Problem: Was ist (noch) erforderlich? z.B. Verwendung von Fotos auf der Internetseite, Weitergabe der E-Mail-Adresse an Geschäftspartner oder Urlaubs-/Krankheitsvertretung durch Mitarbeiter?
- Probleme entstehen in der Regel bei einem Mitarbeiter, der im Unfrieden ausscheidet. Hier drohen zukünftig die dargestellten Rechtsfolgen

- Besonderer Erlaubnistatbestand: Betriebsvereinbarungen
- Geeignet, um die besonderen Anforderungen an den Datenschutz im Arbeitsverhältnis kollektiv zu regeln
- Wichtig: Anpassung der bestehenden Betriebsvereinbarungen an die DSGVO!

Herzlichen Dank für Ihre Aufmerksamkeit!

- Thomas Prehn: prehn@alpmann-froehlich.de

  Tel: 02572 87525
- Martin Breinlich: breinlich@alpmann-froehlich.de

  Tel: 05971 801610

- Weitere Informationen: www.alpmann-froehlich.de