DS-GVO – NEUE RISIKEN UND PFLICHTEN

Notwendige Umstrukturierung der Datenschutzorganisation

MORGENSTERN
Rechtsanwaltsgesellschaft mbH
IT-Recht | Medien | e-Commerce

MORGENSTERN
consecom GmbH
IT-consulting | Datenschutz | Datensicherheit

Gesetze

DS-GVO	Datenschutzgrundverordnung
BDSG	Bundesdatenschutzgesetz
TMG	Telemediengesetz
TKG	Telekommunikationsgesetz
LDSG	Landesdatenschutzgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
StPO	Strafprozessordnung

Inhalt

I. Rechtliche Ausgangsposition

1. BDSG, TMG, TKG, LDSG, UWG, StPO
2. Verbot mit Erlaubnisvorbehalt
   1. Einwilligung
   2. Gesetzliche Ermächtigungsgrundlage
3. Verschiedene allgemeine Grundsätze
   1. Zweckbindung
   2. Transparenz
   3. Datenvermeidung und Datensparsamkeit
   4. Bestimmtheitsgrundsatz

Inhalt

I. Rechtliche Ausgangsposition

4. Dokumentationspflichten
   1. Verfahrensverzeichnisse
   2. Getroffene technisch-organisatorische Maßnahmen
   3. Vorabkontrolle durch den Datenschutzbeauftragten
   4. Rechtmäßigkeitsprüfungen durch den Datenschutzbeauftragten
5. Auftragsdatenverarbeitung
   1. Auswahl des Auftragnehmers
   2. Schriftlicher Vertrag nach § 11 BDSG
6. Betroffenenrechte

Inhalt

II. DS-GVO

1. Vereinheitlichung des Datenschutzniveaus in Europa
2. Rechtmäßigkeit der Verarbeitung
    1. Einwilligung
    2. Vertrag
    3. Rechtliche Verpflichtung
    4. Lebenswichtige Interessen
    5. Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt
    6. Wahrung berechtigter Interessen

Inhalt

II. DS-GVO

3. Grundsätze der Datenverarbeitung
    1. Treu und Glauben
    2. Zweckbindung
    3. Datenminimierung
    4. Richtigkeit
    5. Speicherbegrenzung
    6. Integrität und Vertraulichkeit

Inhalt

II. DS-GVO

Inhalt

II. DS-GVO

6. Betroffenenrechte
   1. Transparenz und Modalitäten
   2. Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten
   3. Berichtigung und Löschung
   4. Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall
   5. Beschränkungen
7. Informationspflichten

Inhalt

III. Datenschutz im Unternehmen

1. Ausgangsposition
2. Auftrags(daten)verarbeitung
3. Rechenschaftspflicht und Dokumentation
4. Verzeichnis von Verarbeitungstätigkeiten
5. Datenschutz-Folgenabschätzung
6. Haftungsrisiken
7. Projekt Umsetzung DS-GVO

I. RECHTLICHE AUSGANGSPOSITION

1. BDSG, TMG, TKG, LDSG, UWG, StPO

- Datenschutzrechtliche Vorschriften sind auf mehrere Gesetze verteilt
- Für Unternehmen sind vor allem das BDSG und das TMG relevant
- Landesbehörden müssen sich nach den LDSG richten
- Vorschriften sind zum Teil Jahrzehnte alt und passen nicht mehr zur heutigen Technologie

2. Verbot mit Erlaubnisvorbehalt

- Ausgangspunkt ist das sogenannte Recht auf informationelle Selbstbestimmung
- Kodifizierung in § 4 Abs. 1 BDSG
- Datenschutz ist Persönlichkeitsrechtsschutz
- Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur Zulässig, wenn der Betroffene eingewilligt hat oder eine gesetzliche Ermächtigungsgrundlage dies erlaubt

2. Verbot mit Erlaubnisvorbehalt

1. Einwilligung

- Anforderungen finden sich in § 4a BDSG
- Koppelungsverbot
- Freie Entscheidung des Betroffenen
- Bestimmtheitsgrundsatz
- Grundsätzlich Schriftform
- Elektronische Einwilligung § 13 Abs. 2 TMG
- Sonstige Form des § 28 Abs. 3a BDSG

2. Verbot mit Erlaubnisvorbehalt

2. Gesetzliche Ermächtigungsgrundlage

- § 28 Abs. 1 Nr. 1 BDSG für Vertragsverhältnisse mit dem Betroffenen
- § 28 Abs. 1 Nr. 2 BDSG zur Wahrung berechtigter Interessen der verantwortlichen Stelle
- § 28 Abs. 3 BDSG Listenprivileg bei Werbung
- § 32 BDSG für Beschäftigtenverhältnisse
- § 14 Abs. 1 TMG für Bestandsdaten
- § 15 Abs. 1 TMG für Nutzungsdaten

3. Verschiedene allgemeine Grundsätze

1. Zweckbindung
2. Transparenz
3. Datenvermeidung und Datensparsamkeit
4. Bestimmtheitsgrundsatz

4. Dokumentationspflichten

1. Verfahrensverzeichnisse
2. Getroffene technisch-organisatorische Maßnahmen
3. Vorabkontrolle durch den Datenschutzbeauftragten
4. Rechtmäßigkeitsprüfungen durch den Datenschutzbeauftragten

5. Auftragsdatenverarbeitung

1. Auswahl des Auftragnehmers
2. Schriftlicher Vertrag nach § 11 BDSG

6. Betroffenenrechte

- § 33 BDSG Benachrichtigung des Betroffenen
- § 34 BDSG Auskunft an den Betroffenen
- § 35 BDSG Berichtigung, Löschung und Sperrung von Daten
- § 7 BDSG Schadensersatz

II. DS-GVO

1. Vereinheitlichung des Datenschutzniveaus in Europa

Bisherige Situation in Europa

- Regelungen der einzelnen Mitgliedstaaten basieren auf geltenden EU-Richtlinien
- Richtlinien wurden jeweils in nationales Recht umgesetzt
- Teilweise sehr unterschiedliche Regelungen in einzelnen Mitgliedsstaaten führen zu uneinheitlichem Datenschutzniveau in Europa
- Wegen der fortschreitenden Entwicklung der Technik sind viele Vorschriften veraltet und passen nicht mehr

1. Vereinheitlichung des Datenschutzniveaus in Europa

Zukünftige Situation in Europa

- Ziel der EU ist die Anhebung und Vereinheitlichung des Datenschutzniveaus in Europa
- Dazu wurde am 4. Mai 2016 im Amtsblatt der Europäischen Union die Datenschutzgrundverordnung (DS-GVO) erlassen
- Die DS-GVO ist ab dem 25. Mai 2018 in den EU-Mitgliedsstaaten unmittelbar wirksam und löst sowohl die EU-Datenschutzrichtlinie als auch die national Datenschutzgesetze (z.B. BDSG) ab
- Die DS-GVO enthält diverse Öffnungsklauseln. Die Öffnungsklauseln ermöglichen den Mitgliedsstaaten ergänzende Regelungen zu treffen
- In Deutschland finden sich ergänzende Regelungen im Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG-EU)
- Einheitliche Begriffsdefinitionen in Art. 4 DS-GVO

2. Rechtmäßigkeit der Verarbeitung

- Struktur ist eine andere
- Sämtliche Tatbestände finden sich in Art. 6 DS-GVO
- Einwilligung und Ermächtigungsgrundlage werden nebeneinander genannt
- Eine der genannten Bedingungen muss erfüllt sein, wobei auch mehrere Bedingungen gleichzeitig vorliegen können (das BDSG sieht so etwas nicht vor)

2. Rechtmäßigkeit der Verarbeitung

1. Einwilligung

- Bedingungen für die Einwilligung finden sich in Art. 7 DS-GVO
- Kein grundsätzliches Schriftformerfordernis mehr
- Erwägungsgrund 32: Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist
- Keine Verteilung auf verschiedene Gesetze, TMG wird also in dieser Hinsicht hinfällig
- Beweislast ausdrücklich beim Verantwortlichen
- Widerrufsrecht, wobei die Rechtmäßigkeit der bisherigen Verarbeitung unberührt bleibt

2. Rechtmäßigkeit der Verarbeitung

2. Vertrag

- Äquivalent zu § 28 Abs. 1 Nr. 1 BDSG
- Durchführung eines Vertragsverhältnisses
- Durchführung vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person (also keine vorvertraglichen Maßnahmen, die vom Verantwortlichen ausgehen)
- Für Arbeitsverträge gilt diese Regelung nicht, da der Arbeitnehmerdatenschutz weiterhin vom nationalen Gesetzgeber geregelt werden soll

2. Rechtmäßigkeit der Verarbeitung

3. Rechtliche Verpflichtung
   - Verpflichtende Meldungen an Behörden
   - Auskunftsverlangen einer Behörde
   - Polizeiliche Ermittlungen
4. Lebenswichtige Interessen
   - Verarbeitung zu humanitären Zwecken einschließlich der Überwachung von Epidemien, Naturkatastrophen
   - Notfälle, Bewusstlosigkeit, Drogeneinfluss

2. Rechtmäßigkeit der Verarbeitung

5. Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt

- Kein echter Erlaubnistatbestand, es bedarf einer nationalen Rechtsgrundlage

6. Wahrung berechtigter Interessen

- Äquivalent zu § 28 Abs. 1 Nr. 2 BDSG, aber weniger streng
- Interessen des Verantwortlichen oder eines Dritten
- Zentrale Abwägungsklausel der DS-GVO
- Rechtliche, wirtschaftliche oder ideelle Interessen
- Erwägungsgrund 47 sieht Direktwerbung als berechtigtes Interesse vor
- Auffangtatbestand, wenn die Verarbeitung nicht zur Erfüllung eines Vertrags dient

3. Grundsätze der Datenverarbeitung

1. Treu und Glauben
2. Zweckbindung
3. Datenminimierung
4. Richtigkeit
5. Speicherbegrenzung
6. Integrität und Vertraulichkeit

4. Dokumentationspflichten

1. Verzeichnis über Verarbeitungstätigkeiten
   - Art. 30 DS-GVO mit ähnlichen Anforderungen wie §§ 4e S. 1, 4g Abs. 2 BDSG
2. Getroffene technisch-organisatorische Maßnahmen
   - Art. 32 DS-GVO konkretisiert die Anforderungen
   - Teile der bisherigen Dokumentation gemäß § 9 BDSG und der dazugehörigen Anlage können aber übernommen werden
   - Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten

4. Dokumentationspflichten

3. Datenschutz-Folgenabschätzung und vorherige Konsultation
   - Art. 35 DS-GVO als Äquivalent der Vorabkontrolle nach § 4d Abs. 5 BDSG
   - Zusätzlich aber Folgenabschätzung im Hinblick auf potenzielle Schadszenarien
   - Konsultationspflicht im Falle eines nicht eingedämmten Risikos, Aufsichtsbehörde gibt dann Empfehlung ab
4. Rechtmäßigkeitsprüfungen durch den Datenschutzbeauftragten
   - Art. 39 DS-GVO
   - Prüfung und Überwachung, Aussprechen von Empfehlungen
5. Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO

5. Auftragsverarbeitung

1. Auswahl des Auftragnehmers
   - Berücksichtigung der getroffenen technisch-organisatorischen Maßnahmen
2. Separater Vertrag
   - Muss nicht mehr schriftlich sein
3. Auftraggeber- und Auftragnehmerpflichten
   - Nach dem BDSG treffen ausschließlich den Auftraggeber bestimmte Pflichten
   - Dies ändert sich mit der DS-GVO
   - Erweiterte Dokumentationspflichten für den Auftragnehmer

6. Betroffenenrechte

1. Transparenz und Modalitäten
2. Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten
3. Berichtigung und Löschung
4. Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall
5. Beschränkungen

7. Informationspflichten

- Umfangreiche Informationspflichten
- Betroffene müssen im Gegensatz zur jetzigen Rechtslage ohne Aufforderung informiert werden (unabhängig von Auskunftsansprüchen)
  - Bei der Erhebung von personenbezogenen Daten über das Internet muss der Betroffene z.B. bei der Erhebung, d.h. direkt bei den Eingabefeldern über den Zweck der Erhebung informiert werden
- Prozesse müssen offengelegt werden
- Relevant gerade bei Datenerhebungen über Apps und Webseiten
- Bewerbermanagement muss transparent ausgestaltet werden

III. DATENSCHUTZ IM UNTERNEHMEN

1. Ausgangsposition

- Ausgangsposition bewerten
- Besonderheiten erkennen
- Schwerpunkte setzen

2. Auftrags(daten)verarbeitung

- Derzeit ist nur der Auftraggeber verantwortlich
- Das ändert sich mit der DS-GVO, ab dem 25.05.2018 obliegen auch den Auftragnehmern gewisse Pflichten
- Vertragsverhältnisse müssen glattgezogen werden (z.B. Webseite, IT-Dienstleister, Datenvernichtung)

3. Rechenschaftspflicht und Dokumentation

- Dokumentationspflicht soll Bewusstsein schärfen
- Regelungsbedürftige Bereiche sollen erkannt werden (IT-Richtlinie)
- Rechtmäßigkeitsprüfungen im Hinblick auf die stattfindende Datenverarbeitung
- Umgang mit Mitarbeiterdatenschutz (E-Mail-Konten, Privatnutzungsverbot)
- Nachweispflicht gegenüber der Aufsichtsbehörde
- Die Umsetzung von Maßnahmen muss dokumentiert werden
- Laufende Überprüfung der Wirksamkeit, Implementierung in Abläufe und Verfahren (Schnittstelle Compliance und IT-Sicherheit)

3. Rechenschaftspflicht und Dokumentation

- Informationspflichten sind zu berücksichtigen und konkret auszugestalten
  - Zusammenspiel mit Datenschutzerklärung
- Abläufe für Anfragen
- Abläufe für Meldung bei Aufsichtsbehörde (Nachfolgeregelung zu § 42a BDSG)
  - Krisenaktionsplan bei meldepflichtigen Datenschutzverletzungen
- Löschkonzept
  - Zusammenspiel mit den Verzeichnissen über Verarbeitungstätigkeiten

4. Verzeichnis von Verarbeitungstätigkeiten

- Wichtiger Baustein für die Rechenschaftspflicht
- Sämtliche Verarbeitungstätigkeiten sind zu identifizieren und zu dokumentieren
- Begriff ist nicht gesetzlich definiert, eine Verarbeitungstätigkeit kann ein Vorgang (z.B. Bewerbermanagementprozess) oder z.B. auch eine bestimmte Softwareanwendung sein (Überschneidungen sind möglich)
- Relevant sind die verarbeiteten personenbezogenen Daten, die Betroffenen und vor allem die Zweckbeschreibung
- Die Pflicht zum Führen der Verzeichnisse ergibt sich bislang aus §§ 4g Abs. 2, 4e S. 1 BDSG

4. Verzeichnis von Verarbeitungstätigkeiten

- Ab dem 25.05.2018 gilt Art. 30 DS-GVO
- Inhalte sind ähnlich
- Erstellung der Verzeichnisse bedarf der Analyse der stattfindenden Prozesse in den einzelnen Abteilungen (z.B. welche Software wird genutzt, wer ist konkret zugriffsberechtigt, gibt es örtliche Besonderheiten, welche Auftrags(daten)verarbeiter sind beteiligt?)
- Erstellung der Verzeichnisse ist mit nicht unerheblichem Aufwand verbunden, je nachdem, wie viele Dienstleister oder Konzernunternehmen involviert sind
- Von Bedeutung ist auch die Löschung von Daten (Aufbewahrungsfristen, Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff)

5. Datenschutz-Folgenabschätzung

- Datenverarbeitungen, die mit besonderen Risiken für die Betroffenen verbunden sind, müssen bisher einer sogenannten Vorabkontrolle nach § 4d Abs. 5 BDSG unterzogen werden
- Klassische Fälle sind die Videoüberwachung, die Zeiterfassung, die Speicherung von Bewegungsdaten oder auch die Verarbeitung besonderer Arten personenbezogener Daten (solange diese nicht zwingend für die Vertragserfüllung benötigt werden wie z.B. bei einem Behandlungsvertrag)

5. Datenschutz-Folgenabschätzung

- Die neue Datenschutz-Folgenabschätzung ist im Prinzip eine Vorabkontrolle mit dem zusätzlichen Erfordernis der Beurteilung möglicher Schadszenarien
- Man muss sich überlegen, welchen potenziellen Schaden eine bestimmte Datenverarbeitung auslösen könnte
- Auf dieser Basis muss dann beurteilt werden, ob weitere technisch-organisatorische Maßnahmen zu treffen sind
- Bei einer negativen Datenschutz-Folgenabschätzung muss sogar die Aufsichtsbehörde informiert und befragt werden

6. Haftungsrisiken

- Bußgelder pro Verstoß liegen derzeit bei 50.000,00 EUR und 300.000,00 EUR
- DS-GVO sieht 10.000.000,00 EUR / 20.000.000,00 EUR oder im Fall eines Unternehmens von bis zu 2 % / 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs vor
- Je nachdem, um welchen Verstoß es sich handelt
- Die DS-GVO enthält deutlich mehr Bußgeldtatbestände
- Allein die Verletzung von Informationspflichten ist schon bußgeldbewehrt, das BDSG sieht so etwas nicht vor
- Überprüfung für die Aufsichtsbehörden wird einfacher (ein Blick auf die Webseite kann für die Verhängung eines Bußgeldes genügen)

6. Haftungsrisiken

- Umsetzung der neuen Vorgaben kann nur in enger Zusammenarbeit mit den Mitarbeitern erfolgen
- Bereits vorhandene Prozessbeschreibungen sind hilfreich
- Konkrete Fragen zu einzelnen Verarbeitungsvorgängen sind jedoch unerlässlich
- Es können neue Fragen auftauchen

7. Projekt Umsetzung DS-GVO

- Aufbau einer EU-weiten Datenschutzorganisation
- Schnittstellen zu IT-Sicherheitsanalysen und Compliance-System
- Minimierung von Haftungsrisiken
- Projekt muss bis zum 25.05.2018 (weitgehend) abgeschlossen sein

7. Projekt Umsetzung DS-GVO

- Ziele und (Neben)Effekte
  - Synergien
  - Interne Transparenz
  - Awareness und internes Know-How
  - Erhöhung der Effektivität
  - Optimierungspotenzial erkennen und umsetzen
  - Positive Energien

MORGENSTERN
Rechtsanwaltsgesellschaft mbH
IT-Recht | Medien | e-Commerce

MORGENSTERN
consecom GmbH
IT-consulting | Datenschutz | Datensicherheit

Vielen Dank für Ihre Aufmerksamkeit

MORGENSTERN
Rechtsanwaltsgesellschaft mbH

Maximilianstraße 49
67346 Speyer

Telefon 0 62 32. 100 119 - 0
Telefax 0 62 32. 100 119 - 29

mail@m-kanzlei.de
www.m-kanzlei.de