Workshop Datenschutzgrundverordnung

Vortragende: Jasmina Opawa

Inhalt

Teil 1:

- Grundzüge des Datenschutzrechts
  - Begriffsbestimmungen
- Datenschutzbeauftragter
- Pflichten aus der DSGVO
- Rechte der Betroffenen
- Verfahren und Kontrollen, Strafmaßnahmen
- Zusammenfassung: Welche Schritte sind konkret zu setzen?

Teil 2:

- Informationssicherheit

1) Grundzüge des Datenschutzrechts

Grundrecht auf Datenschutz:

Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, insoweit ein schutzwürdiges Interesse daran beseht.

§ 1 Abs. 1 DSG 2018

Verfassungsbestimmung

1) Grundzüge des Datenschutzrechts

- EMRK: Europäische Menschenrechtskonvention (Artikel 8 Recht auf Achtung des Privat- und Familienlebens, das Recht auf Wohnung und der Schutz der Korrespondenz
- Datenschutzrichtlinie: Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Vorgänger der DSGVO
- Datenschutzgesetze: Jedes Europäische Land hatte die Vorgaben der Datenschutzrichtlinie in die nationale Rechtssprechung umgesetzt. Weitgehend unterschiedlich, datenschutzrechtliches „Patchwork“
- Datenschutzbehörde: unabhängige Aufsichtsbehörde

1) Grundzüge des Datenschutzrechts

Datenschutzgrundverordnung (DSGVO)

- Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten
  - unmittelbar anwendbar
  - Inkrafttreten: 25. Mai 2018
  - EU-Bezug: Niederlassung, betroffene Personen
  - automatisierte Verarbeitung
  - nicht automatisierte Verarbeitung in Dateisystem (=strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind)
  - Art. 2 und Art. 3

Begriffsbestimmungen

- Daten
- Besondere Kategorien personenbezogener Daten
- Verarbeitung
- Grundsätze der Verarbeitung
- Einwilligung

Begriff Daten

Personenbezogene Daten:

- sind alle Informationen, die sich
  - auf eine identifizierte oder
  - identifizierbare
  - natürliche Person

beziehen.

- Beispiele: Name, Adresse, Geburtsdatum,

Begriff „besondere Kategorie personenbezogener Daten“

Sensible Daten:

DSGVO: besondere Kategorien personenbezogener Daten

DSG 2000: sensible Daten

- rassische und ethnische Herkunft
- politische Meinung
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit (körperlich, geistig)
- Biometrische und genetische Daten (neu!)
- Sexualleben

Begriff Verarbeitung

Automatisiert (EDV) oder **nicht automatisiert** (soweit in einem Dateisystem erfasst: Karteien in Papierform)

Die Verarbeitung von Daten umfasst

- Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen und Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreitung oder andere Form der Bereitstellung, Abgleichen oder Verknüpfen, Einschränken, Löschen oder Vernichten.

Art.4 Z.2

Grundsätze der Verarbeitung

a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

b) Zweckbindung

c) Datenminimierung

d) Richtigkeit

e) Speicherbegrenzung (Löschpflichten beachten: z.B. BAO oder UGB)

f) Integrität und Vertraulichkeit

Art. 5

ad a) Rechtmäßigkeit

- Einwilligung der betroffenen Person für einen oder mehrere Zwecke (nachweislich, schriftlich, jederzeitiger Widerruf möglich)
- Erfüllung eines Vertrages oder vorvertragliche Maßnahmen auf Anfrage der betroffenen Personen
- rechtliche Verpflichtung des Verantwortlichen
- lebenswichtige Interessen der betroffenen Personen oder einer anderen natürlichen Person
- Aufgabe des öffentlichen Interesse
- berechtigtes Interesse des Verantwortlichen oder Dritten, sofern nicht Interessen der betroffenen Person überwiegen

Art. 6

ad b) Zweckbindung

- für festgelegte, eindeutige und legitime Zwecke
- keine Weiterverarbeitung in einer Weise, die nicht mit diesen Zwecken vereinbar ist
- Ausnahme: Archivzwecke im öffentlichen Interesse, wissenschaftliche oder historische Forschungszwecke, statistische Zwecke

ad c) Datenminimierung

- personenbezogene Daten müssen dem Zweck angemessen sein
- erheblich und
- auf das notwendige Maß beschränkt

ad d) Richtigkeit

- sachlich richtig
- auf dem neuesten Stand
- es sind alle Maßnahmen zu treffen, um Daten die im Hinblick auf den Zweck unrichtig sind, unverzüglich gelöscht oder berichtigt werden

ad e) Speicherbegrenzung

- Speicherung nur so lange, wie für die Zwecke erforderlich (gesetzl. Aufbewahrungsfristen beachten BAO, UGB,…) Dies erfordert jedoch nicht die Erhaltung des kompletten Datensatzes, sondern nur die Erhaltung jener Daten, die für die gesetzliche Nachweisführung notwendig sind!

- Ausnahmen: Archivzwecke etc. siehe b) (Archivzwecke im öffentlichen Interesse!)

ad f) Integrität und Vertraulichkeit

- angemessene Sicherheit der personenbezogenen Daten:
- umfasst Schutz vor unbefugter und unrechtmäßiger Verarbeitung
- und vor unbeabsichtigtem Verlust, Zerstörung oder Beschädigung
- durch geeignete technische und organisatorische Maßnahmen (siehe Teil 2 des Vortrages)

Rechenschaftspflicht:

- Der Verantwortliche ist für die Einhaltung der Grundsätze verantwortlich und muss dies auch nachweisen können.

Einwilligung

„Einwilligung“ muss freiwillig für den bestimmten Fall gegeben werden

- in informierter und unmissverständlicher Weise
- Willensbekundung zur Verarbeitung der Daten (schriftlich, elektronisch oder mündlich- schwer nachvollziehbar!)
- Dient die Verarbeitung mehreren Zwecken, für jeden Zweck der Verarbeitung eine gesonderte Einwilligung nötig
- „Ausdrückliche“ Einwilligung nur bei Verarbeitung sensibler Daten erforderlich

Kind (Art 8 Abs 1)

- DSGVO setzt Altersgrenze von 16 Jahren fest.
- EU-Mitgliedstaaten können aber niedrigere Altersgrenzen vorsehen, allerdings nicht unter vollendetes 13. Lebensjahr

- DSG neu, Altersgrenze mit vollendetem 14. Lebensjahr! Darunter muss Einwilligung der Eltern eingeholt werden!

2) Datenschutzbeauftragter

ist zu benennen:

- bei Verarbeitung von einer Behörde oder öffentlichen Stelle (außer Gerichte)

- wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund
  - ihrer Art
  - ihres Umfanges und/oder
  - ihrer Zwecke
  - eine umfangreiche regelmäßige und systematische Überwachung

- wenn die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten (=sensible Daten) oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten besteht.

2) Datenschutzbeauftragter

Aufgaben:

- zentrale Informationsstelle für Datenschutz.
- Kontrollaufgaben bzgl der Einhaltung der Datenschutzvorschriften
- Kontaktaufgaben als zentrale Ansprechperson für die Datenschutzbehörde
- Schulungsaufgaben zur Ausbildung und Sensibilisierung der MA im Unternehmen

Artikel 37 enthält einige grundsätzliche Aussagen zur Qualifikation des Datenschutzbeauftragten

- Beruflicher Qualifikation, vor allem des Fachwissens auf dem Gebiet des Datenschutzrechts und Datenschutzpraxis
- Fähigkeiten zur Erfüllung der Aufgaben einesDatenschutzbeauftragten
- Haftung: haftet lediglich nach den allgemeinen Regeln, nicht aber gegenüber der Behörde für die Strafen

3) Pflichten aus der DSGVO

Hauptfragen zur DSGVO

- Bin ich von der DSGVO betroffen?

Ja: Alle österreichischen Unternehmen jeder Branche auch ARGE, Vereine, Ärzte, KMU, EPU, Schulen etc.

- Gibt es noch Meldepflichten bei der Datenschutzbehörde?

Nur in 2 Fällen: bei Datenleck (data breach) und wenn Datenverarbeitung sehr riskant ist und Ergebnis der Datenschutz-Folgenabschätzung – Risiko kann nicht eingedämmt werden

- Was ist das Verarbeitungsverzeichnis?

Das Verarbeitungsverzeichnis ist ein Protokoll aller datenschutzrelevanter Vorgänge im Betrieb. Ausnahme von der Verzeichnisführung nur wenn "Verarbeitung nur gelegentlich erfolgt und kein Risiko damit verbunden„

- Wer kann mein Datenschutzbeauftragter sein?

Jeder der Erfahrung mit dem Datenschutz hat, nicht bei Interessenskonflikten wie GF oder IT-Leiter, Rechtsabteilung, etc.

3) Pflichten aus der DSGVO

a) Verzeichnis von Verarbeitungstätigkeiten

- ersetzt DVR-Register
- ab 250 Mitarbeiter obligatorisch
- bis 250 Mitarbeiter
    - wenn Verarbeitung ein Risiko für Rechte und Freiheiten der betroffenen Personen birgt
    - die Verarbeitung nicht nur gelegentlich erfolgt oder
    - besondere Kategorien betroffen sind

Art. 30

3) Pflichten aus der DSGVO

Pflichtangaben:

- Namen und Kontaktdaten des Verantwortlichen
- Zwecke der Verarbeitung
- Kategorien der betroffenen Personen und personenbezogener Daten
- Kategorien der Empfänger
- Übermittlung in ein Drittland
- vorgesehene Fristen der Löschung der Daten
- wenn möglich: allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Das Verzeichnis wird auf Anfrage der Datenschutzbehörde zur Verfügung gestellt.

3) Pflichten aus der DSGVO

b) Meldung der Verletzung des Schutzes personenbezogener Daten an die Datenschutzbehörde (Datenpanne, data leak)

- bei Verletzung des Schutzes personenbezogener Daten
- Meldung durch den Verantwortlichen
- binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde
- es sei denn: die Verletzung führt voraussichtlich nicht zu einem Risiko für Rechte und Freiheiten natürlicher Personen

3) Pflichten aus der DSGVO

Inhalt der Meldung:

- Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten
- Namen und Kontaktdaten des Datenschutzbeauftragten
- Beschreibung der wahrscheinlichen Folgen
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung, Abmilderung der Folgen
- Pflicht zur Dokumentation
- besteht ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen: unverzügliche Benachrichtigung der betroffenen Person

Art. 33 und 34

3) Pflichten aus der DSGVO

c) Datenschutz-Folgenabschätzung:

- bei Verwendung neuer Technologien

4) Rechte der Betroffenen

- Recht auf Auskunft
- Recht auf Richtigstellung
- Recht auf Löschung
- Recht auf Einschränkung der Verarbeitung

4) Rechte der Betroffenen

Recht auf Auskunft

Bestätigung, ob folgende Daten verarbeitet werden

- Verarbeitungzwecke
- Datenkategorien
- Kopie (z.B. Ausdruck) der verarbeiteten Dateninhalte
- Datenempfänger

4) Rechte der Betroffenen

Recht auf Auskunft (Frist zur Auskunftserteilung : 1 Monat, Verlängerung auf 3 Monate möglich, Recht auf Auskunft über eigene Daten – Ausweiskopie, wenn Identität nicht feststeht, oder Negativauskunft, wenn keine Daten vorhanden)

- Bestehen eines Berichtigungs-, Löschungs- oder Widerspruchsrechts
- Bestehen eines Auskunftsrechts bei der Beschwerdebehörde
- Verfügbare Information über Datenherkunft

4) Rechte der Betroffenen

Recht auf Berichtigung

- Recht auf Vervollständigung von Daten (=neu)
- Frist: 1 Monat

4) Rechte der Betroffenen

Recht auf Löschung umfasst auch das Recht auf Vergessenwerden

- Wegfall des Verarbeitungszwecks

4) Rechte der Betroffenen

Recht auf Vergessenwerden

- Veröffentlichung (z.B. im Internet) durch den Verantwortlichen
- Bei Löschung: alle angemessenen Maßnahmen zur Entfernung von Links, Kopien etc.
- Information an Suchmaschinenbetreiber

Frist für Löschung : 1 Monat (max. 3 Monate)

4) Rechte der Betroffenen

Recht auf Einschränkung der Verarbeitung

- zeitlich eingeschränktes Recht
- Richtigkeit der Daten wird bestritten, der Betroffene lehnt die Löschung ab
- der Betroffene benötigt die Daten
- der Betroffene hat Widerspruch eingelegt

5) Kontrollen und Strafbestimmungen

Befugnisse der Datenschutzbehörde

- Untersuchungsbefugnis: auch Betretungsrecht bestimmter Räumlichkeiten
- Abhilfebefugnis: Anordnungen und Verwaltungsstrafen
- Genehmigungs- und Beratungsbefugnisse

5) Kontrollen und Strafbestimmungen

- Geldbußen: als Verwaltungsstrafen gegen Unternehmen oder Einzel-personen
- Keine Sonderbestimmungen für gemeinnützige Vereine
- Verwarnung ist möglich
- Leichte Verstöße: max. 10 Millionen Euro oder 2% vom Vorjahresumsatz
- Schwere Verstöße: max. 20 Millionen Euro oder 4 % vom Vorjahresumsatz
- Schadenersatz bei materiellen oder immateriellen Schäden

6) Konkrete Schritte

- Erfassung des Bestandes an Daten (welche Arten von Daten werden verarbeitet, wer greift zu, an wen werden sie übermittelt,….)
- Maßnahmen der Informationssicherheit (am besten „best practices“ bei den Anbietern erfragen, Verschlüsselung implementieren, Nachvollziehbarkeit, Zugriffsrechte definieren, keine gemeinsamen Nutzerkonten, räumliche Sicherheit v. Servern, etc.)
- Zuständigkeit – Datenschutzbeauftragter und Informationsicherheit
- Verzeichnis der Verarbeitung (vlcht. bestehenden DVR- Eintrag downloaden, überarbeiten und in das DSGVO-konforme Format bringen)
- Folgenabschätzung speziell für sensible Daten durchführen, Maßnahmen ableiten (siehe Informationssicherheit)
- Ablauf für Auskünfte von Betroffenen sowie Prozess für eine mögliche Verletzung des Schutzes personenbezogener Daten definieren (wer ist im Falle zu informieren, Zeitrahmen beachten)

7) Informationssicherheit

3 Grundsätze:

- **Vertraulichkeit**: Daten dürfen nur von autorisierten Nutzern verarbeitet oder übertragen werden.
- **Verfügbarkeit**: Schutz vor Systemausfällen oder ähnlichem, innerhalb einer im Voraus festgesetzten Zeitspanne müssen die Daten wieder verfügbar sein.
- **Integrität**: Daten dürfen nicht verändert werden, Änderungen müssen nachvollziehbar sein.

Maßnahmen – ISO 27002

7) Informationssicherheit

14 Kapitel:

1. Informationssicherheitsrichtlinien

- Security Policy – Vorgaben der Geschäftsleitung in Übereinstimmung mit geschäftlichen Anforderungen, Gesetzen und Vorschriften
  - Definition von Informationssicherheit, Ziele und Grundsätze
  - Zuordnung von Verantwortlichkeiten
  - Prozesse für Abweichungen und Ausnahmen

7) Informationssicherheit

- Verweis auf themenspezifische Richtlinien
  - Zugangssteuerung
  - physische und umgebungsbezogene Sicherheit

- Richtlinien für Endanwender: zulässiger Gebrauch von Hard- und Software, aufgeräumte Arbeitsumgebung und Bildschirmsperren, Informationsübertragung, Mobilgeräte und Telearbeit, Einschränkungen für Softwareinstallation und -verwendung

7) Informationssicherheit

2. Organisation der Informationssicherheit

- Interne Organisation: Rollen und Verantwortlichkeiten
- Aufgabentrennung: Systemadministration, Überwachung, Leitungsaufsicht
- Kontakte mit Behörden, Datenschutzbehörde, Auskünfte
- Kontakte mit speziellen Interessensgruppen, sicherheitsorientierten Fachverbänden

7) Informationssicherheit

Mobilgeräte und Telearbeit:

- Mobilgeräte: Smartphone, Tablet, Laptop, Notebook
- Richtlinie, um die Risiken zu handhaben
- Registrierung von Smartphones
- Anforderungen an den physischen Schutz (Auto, Hotel..)
- Verwendung an öffentlichen Plätzen (WLAN, Passwörter, Verschlüsselung, Authentifizierung).
- Einschränkung von Softwareinstallationen

7) Informationssicherheit

- Verbindungseinschränkungen zu Informationsdiensten, Webdiensten
- Maßnahmen zum Zugang zu Mobilgeräten
- Verschlüsselungsverfahren
- Remote-Deaktivierung, Löschung oder Sperrung
- Backups
- Trennung von privater und geschäftlicher Sphäre – durch Softwareunterstützung
- Endnutzervertrag zur Regelung aller Anforderungen

7) Informationssicherheit

3. Personalsicherheit

- Sicherheitsüberprüfung
- Beschäftigungs- und Vertragsbedingungen: Vertraulichkeitserklärung, Geheimhaltungsvereinbarung
- Informationssicherheitsbewusstsein, - ausbildung und – schulung
- Maßregelungsprozess
- Beendigung und Änderung der Beschäftigung

7) Informationssicherheit

4. Verwaltung von Werten bzw. Beständen

Was sind Werte (Assets) im Sinne der Norm:

- Hardware: Computer, Laptop, Drucker, Modem, Speichermedien
- Software
- Datenbanken, Verträge, Dokumentationen, Schulungsunterlagen
- Strom, Heizung, räumliche Gegebenheiten
- Personal: Qualifikationen

7) Informationssicherheit

Ziel: Erfassung aller Bestände und Festlegung der Verantwortlichkeit

A) Inventarisierung: Aufstellung aller Bestände

B) Festlegung von Zuständigkeit: zulässiger Gebrauch, Rückgabe

C) Klassifizierung von Information: es wird sichergestellt, dass ein angemessenes Schutzniveau entsprechend der Bedeutung in der Organisation hergestellt wird

7) Informationssicherheit

Informationsklassifizierung

z.B. 4 Stufen (optional auch 3 Stufen möglich):

I. Offenlegung ist gefahrlos möglich

II. Offenlegung führt zu geringfügigen betrieblichen Unannehmlichkeiten

III. Offenlegung hat signifikante, kurzfristige Auswirkungen auf den Betriebsablauf oder taktische Ziele

IV. Offenlegung hat schwerwiegende Auswirkungen auf langfristige strategische Zielsetzungen und gefährdet den Bestand der Organisation

7) Informationssicherheit

- Kennzeichnung der Bestände entsprechend der Klassifizierung
- Zugangsbeschränkungen entsprechend der Klassifizierung
- Liste von befugten Empfängern
- Kopierschutz oder
- Kennzeichnung von Kopien für den Empfänger

7) Informationssicherheit

Wechseldatenträger (z.B. USB-Sticks)

- Löschen von nicht mehr benötigten Inhalten
- Genehmigungspflicht für das Entfernen von Wechseldatenträger aus der Organisation
- sichere Aufbewahrung
- Verschlüsselungsverfahren
- Risiko des Verlustes von Daten: Umspeichern auf neue Datenträger bevor sie unlesbar werden
- Erstellung von Kopien
- Registrierung der Wechselmedien
- Überwachung der Verwendung von Wechseldatenträger

7) Informationssicherheit

- Entsorgung von Datenträgern (Externer Dienstleister: angemessene Sicherheitsmaßnahmen und Erfahrung Protokollierung bei sensiblen Daten)
- Transport von Datenträgern- zuverlässige Transport- oder Kurierdienste, Protokollierung
- Anwendung von formalen Verfahren
- Sichere Lagerung und Entsorgung: Shreddern, Verbrennen, sicheres Löschen
- Ermittlung der Daten, die so vertraulich sind, dass sie sicher entsorgt werden müssen
- Oder alle Datenträger sicher entsorgen (wenn das einfach ist)

7) Informationssicherheit

Weitere Kapitel der Norm 27002

- Zugangssteuerung
- Kryptographie
- Physische und umgebungsbezogene Sicherheit
- Betriebssicherheit
- Kommunikationssicherheit
- Anschaffung, Entwicklung und Instandhaltung von Systemen
- Lieferantenbeziehungen
- Handhabung von Informationssicherheitsvorfällen
- Informationssicherheit beim Business Continuity Management
- Compliance

EXKURS NEWSLETTER

§ 107 Abs. 2 TKG:

Zusendung elektronischer Post (auch SMS) ist ohne vorherige Einwilligung des Empfängers unzulässig, wenn

- die Zusendung zu Zwecken des Direktmarketings erfolgt und
- an mehr als 50 Empfänger gerichtet ist.

Direktmarketing: darunter ist jede Werbung für ein Produkt oder eine Dienstleistung zu verstehen , nicht z.B. Meinungsforschung

Exkurs: Newsletter

Keine Einwilligung ist notwendig, wenn

- der Absender die Kontaktinformation in Zusammenhang mit dem Verkauf oder einer Dienstleistung an den Kunden erhalten hat und
- die Nachricht für Direktwerbung für eigene ähnliche Produkte erfolgt und
- der Empfänger klar und deutlich die Möglichkeit erhalten hat, die Informationen abzulehnen und
- der Empfänger nicht in der Liste nach § 7 Abs 2 ECG eingetragen ist.

Für Adressen, die vor dem 1. März 2006 erhoben wurden, war die Möglichkeit der Abbestellung nicht Voraussetzung, daher kann an jeden weiterversendet werden, wenn email- Adresse rechtsmäßig erhoben wurde. Bei jeder neuen Email muss aber Möglichkeit zur Abbestellung gegeben sein.

Einwilligung zulässig erheben

Einwilligung kann durch jede Art der Kontaktaufnahme eingeholt werden, die nicht den oben genannten Verboten widerspricht.

- Brief an den Empfänger
- persönlicher Kontakt, bei dem eine zumindest schlüssige (besser schriftliche) Zustimmung des Empfängers für künftigen E-Mailkontakt erteilt und dokumentiert wird
- evtl die Zustimmung über AGB (sehr heikel)
- durch regelmäßigen Kontakt in aufrechten Geschäftsbeziehungen
- jede andere Form einer schlüssigen Zustimmung des Empfängers für künftigen Mailkontakt (ausreichende Dokumentation empfehlenswert)
- jede Zustimmung des Empfängers (zB angekreuztes Zustimmungsfeld auf Webformular, beim Download oder sonstigen Konsum von Angeboten, anlässlich eines Telefon-/ E-Mail-Kontakts, der vom Empfänger ausgeht.)

!!!Einwilligung darf jedoch **nicht** durch verbotene Telefon- E-Mail- oder Faxwerbung eingeholt werden!!!

Weitere Informationen

- Leitfaden der Datenschutzbehörde – www.dsb.gv.at
- Zusammenfassung und weitere Links – www.help.gv.at
- RTR - https://www.rtr.at/de/tk/TKKS_ECGEintrag
- Wirtschaftskammer – www.wko.at
  - Muster eines Verarbeitungsverzeichnisses
  - Online-Tool

Herzlichen Dank
für
IHre Aufmerksamkeit!

Jasmina Opawa

Datenschutzbeauftragte

Email: jasopawa@gmail.com