Wirtschaftskammer Steiermark
RECHTSSERVICE
E rechtsservice@wkstmk.at T 0316/601-601 http://wko.at/stmk

Datenschutz Grundverordnung

Montag, 10. September 2018
14.00 - 17.00 Uhr

Mag. Markus Dörfler LL.M.,
Partner der Höhne, In der Maur & Partner Rechtsanwälte GmbH & Co KG, Wien

WKO STEIERMARK

Die Datenschutz-Grundverordnung

Höhne
In der Maur
& Partner

Rechtsanwälte

Mag. Markus Dörfler
Rechtsanwalt

10.09.2018

Markus Dörfler

1999 - 2005	Synaptic Networks
2006	Mag. iur. Universität Linz
2006 - 2007	Universitätslehrgang für Informationsrecht und Rechtsinformation, Universität Wien
2007	Master of Laws (LL.M.)
2012 - 2016	selbstständiger Rechtsanwalt - in Kooperation mit Höhne, In der Maur & Partner
2016	Partner bei Höhne, In der Maur & Partner Rechtsanwälte

Datenschutzrecht „alt“

- DSG 2000

- Schutzbereich:

personenbezogene Daten

Datenschutzrecht „alt“

- Zweckgebundenheit
- Registrierpflicht (mit Ausnahmen)
- Datensicherheit

Datenschutzrecht „alt“

- Verstöße:

  Verwaltungsstrafe bis zu EUR **25.000,00**

Datenschutzrecht „alt“

- Mein Rat:

Tun Sie nichts

DSGVO

- Sanktion:
  - „wirksam, verhältnismäßig und abschreckend“
- Geldbuße:
  - bis zu EUR 10 Mio (oder 2% des weltweiten Jahresumsatzes)
  - bis zu EUR 20 Mio (oder 4% des weltweiten Jahresumsatzes)
  - zuständig: Aufsichtsbehörde

Rechtsgrundlage

- Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
- In Kraft seit **24.5.2016** (anzuwenden seit 25.5.2018)

Rechtsgrundlage

- Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) In Kraft seit **25.5.2018**
- DSG 2000 idF Datenschutz-AnpassungsG 2018 (BGBl I 120/2017)
- Div. innerstaatliche Rechtsgrundlagen (Öffnungsklauseln): DSFA-AV, 2 Materien-Datenschutz-Anpassungsgesetze, Datenschutz-DeregegulierungsG 2018 etc.

Rechtsgrundlage

- Schutzbereich:

personenbezogene Daten

- ganz oder teilweise automatisierte Verarbeitung

Grundbegriffe

- personenbezogene Daten
- Betroffene Person
- Verantwortlicher
- Auftragsverarbeiter
- Verarbeitung von Daten
- Profiling
- Einwilligungserklärung

Personenbezogene Daten

- „*personenbezogene Daten*“ (Art 4 Z 1 DSGVO) alle Informationen, die sich
  - direkt oder indirekt
  - auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen;
- **Keine** juristischen Personen
- **Keine** Daten von verstorbenen Personen
  - Achtung: Öffnungsklausel

Personenbezogene Daten

- als identifizierbar wird eine natürliche Person angesehen, die insbesondere mittels Zuordnung
  - zu einer Kennung wie einem Namen,
  - zu einer Kennnummer,
  - zu Standortdaten,
  - zu einer Online-Kennung

  oder

Personenbezogene Daten

- als identifizierbar wird eine natürliche Person angesehen, die insbesondere mittels Zuordnung
  - zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind

identifiziert werden kann

Personenbezogene Daten

– „*es gibt kein belangloses Datum*“ (dBVerfG vom 15.12.1983, 1 BvR 209/83)
  - Selbst die Information, dass Person X zwei Arme hat, stellt personenbezogenes Datum dar.
  - Auch statistische Wahrscheinlichkeitsaussagen und nicht völlig abstrakte Prognose- oder Planungswerte, die eine subjektive und/oder objektive Einschätzung zu einer identifizierten oder identifizierbaren Person liefern, weisen einen Personenbezug auf. (Art 29 Datenschutzgruppe Stellungnahme 4/2007 – WP 136,7).

Personenbezogene Daten

- Abgrenzung zu Sachdaten
  - Achtung: IoT
- Die Unterscheidung „*identifizierbar vs indentifiziert*“ ist irrelevant
- Wann ist eine Person identifizierbar:
  - Berücksichtigung aller Mittel
  - Außer: eine Identifizierung ist *praktisch* nicht durchführbar (EuGH vom 12.5.2016 – C-582/14)
  - Auch: rechtswidrige Mittel?

Personenbezogene Daten

- Einzelfälle:
  - IP-Adresse
    - Personenbezogenes Datum
  - Cookies
    - Hängt von den gespeicherten Daten ab

Personenbezogene Daten

- Grundsatz:

Sofern sich Informationen auf eine natürliche Person beziehen, liegen personenbezogene Daten vor

besondere Kategorien von Daten

- besondere Kategorien von Daten (Art 9 DSGVO)
  - die rassische und ethnische Herkunft, politische Meinungen, **religiöse** oder weltanschauliche **Überzeugungen**, die Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten** oder Daten zum Sexualleben oder der sexuellen Orientierung

besondere Kategorien von Daten

- Art 9 (1): „Die Verarbeitung personenbezogener Daten, aus denen die […] religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von […] Gesundheitsdaten […] ist untersagt.“

Verantwortlicher

- Verantwortlicher (Art 4 Z 7 DSGVO):

„*Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.*“

Verantwortlicher

- „wer ist für die Einhaltung der Datenschutzbestimmungen verantwortlich“
- Natürliche oder juristische Personen, Behörden, Einrichtungen und sonstige Stellen
- Entscheidungsbefugnis über den Zweck der Datenverarbeitung („Ob“, „Wofür“, „Wieweit“)
- Mitarbeiter sind keine Verantwortliche

Auftragsverarbeiter

- Auftragsverarbeiter (Art 4 Z 8 DSGVO):
  - Verarbeitung im Auftrag des Verantwortlichen
  - Beispiel: Anbieten von Internetdiensten (Hosting)
  - Voraussetzung für eine wirksame Auftragsverarbeitung
  - „Wer entscheidet über Zwecke und Mittel der Verarbeitung personenbezogener Daten“

Auftragsverarbeiter

- Pflichten:
  - Vertragsabschluss (Achtung: Geldbuße)
  - Einfordern von Weisungen
    - Auch: Äußern von Bedenken
    - Bei Abweichungen zum Vertragsgegenstand: Der Auftragsverarbeiter wird Verantwortlicher
  - Zertifizierung
  - Verschwiegenheit

Auftragsverarbeiter

- Pflichten (Fortsetzung):
  - Dokumentation von Unternehmensprozesse
    - Betroffenenrechte
    - Rückgabe und Löschung
    - Meldung von Datenverlusten
  - Bestellung eines Datenschutbeauftragten
  - Führen eines Verarbeitungsverzeichnisses
  - Organisation der Unter-Auftragsverarbeiter

Auftragsverarbeiter

- Pflichten (Fortsetzung):
  - Meldepflicht an den Verantwortlichen
  - Informationspflicht an den Verantwortlichen
  - Haftung
    - Gegenüber dem Betroffenen (Art 82 Abs 1 DSGVO)
    - Passiv Klagslegitimiert (Art 79 DSGVO)
  - Geldbuße (Art 83 Abs 4 lit a DSGVO)

Auftragsverarbeiter

- Stichwort:

  schriftliche
  Auftragsverarbeitervereinbarung
- Aber: Standardvertragsklauseln
- Fragen:
  - Steuerberater
  - Rechtsanwälte

Profiling

- Profiling (Art 4 Z 4 DSGVO):
  - 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…

Profiling

- …insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
- „Persönlichkeitsbewertung“
- Beispiel: Credit-Scoring

Einwilligung

- Einwilligung (Art 4 Z 11 DSGVO):
  - Zustimmung der betroffenen Person, dass personenbezogene Daten über die betroffene Person verarbeitet werden dürfen.

Einwilligung

- Voraussetzungen:
  - Freiwilligkeit
    - Koppelungsverbot (?)
  - Bestimmtheit
    - Zweckbindung
  - Informiertheit
    - Abschätzbarkeit der Auswirkungen
  - Einwilligungsbewusstsein
    - Keine vorangekreuzten Häkchen

Verarbeiten

- Verarbeiten (Art 4 Z 2 DSGVO):
  - jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie …

Verarbeiten

– …das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

Datensicherheit

- Datensicherheit (Art 30 DSGVO):

Abzuwägen sind:

- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände und Zweck der Verarbeitung
- Eintrittswahrscheinlichkeit und Schwere des Risikos

Zu ergreifen sind:

- geeignete technische und organisatorische **Maßnahmen**

Verarbeitung

- Rechtmäßigkeit der Verarbeitung (Art 6 DSGVO):
  - Einwilligung
  - Erfüllung eines Vertrags
  - Erfüllung einer rechtlichen Verpflichtung
  - Lebenswichtige Interessen des Betroffenen
  - Wahrnehmung einer Aufgabe im öff. Interesse
  - Berechtige Interessen des Verantwortlichen

Datenminimierungspflicht

- Daten dürfen nur für gewisse Zwecke verarbeitet werden
- Die Verarbeitung muss auf das für den Zweck der Verarbeitung notwendige Maß beschränkt werden.
- Daher: sollten Daten für den Zweck nicht notwendig sein, sind sie zu löschen.

Datengeheimnis

- § 6. (1) DSG: Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, **geheim zu halten**, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (**Datengeheimnis**).

Datengeheimnis

- § 6. (2) DSG: Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer **ausdrücklichen Anordnung** ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, **diese vertraglich zu verpflichten**, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

Datengeheimnis

- § 6. (3) DSG: Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses **zu belehren**.
- Kein Nachteil aus der Weigerung, eine unzulässige Datenübermittlung durchzuführen

Umsetzung und Rechtsfolgen

Verfahrensverzeichnis

- Verzeichnis von Verarbeitungstätigkeiten (Art 30 DSGV) – „Verfahrensverzeichnis“
  - Anknüpfungspunkt: der Zweck der Verarbeitungstätigkeit
  - Dokumentation (auch elektronisch)
  - Jederzeitige Verfügbarkeit (Einsichtsrecht der Behörde)
  - Aktualisierungspflicht

Verfahrensverzeichnis

- Inhalt:
  - Namen und Kontaktnamen des Verantwortlichen (samt Ansprechpartner)
  - Zweck der Verarbeitung
    - Dem Verantwortlichen muss der Zweck der Verarbeitung bewusst sein, um die Rechtsmäßigkeit der Verarbeitung bewerten zu können.

Verfahrensverzeichnis

- Inhalt (Fortsetzung):
  - Kategorien der betroffene Personen und der personenbezogenen Daten
    - Beispiele: „Beschäftigte“, „Kunden“
    - Besondere Kategorien von Daten, strafrechtlich relevante Daten
  - Kategorien von Empfänger
    - Daten wurden bereits oder werden offengelegt
    - „eine realistische Möglichkeit der Weitergabe besteht“
    - Beispiele: „Logistikdienstleister“

Verfahrensverzeichnis

- Inhalt (Fortsetzung):
  - Benennung von Drittländern
  - Fristen für die Löschung
    - Abstrakte Dauer der Speicherung
  - Beschreibung der technischen und organisatorischen Maßnahmen
    - Datensicherheit
    - Detailgrad: die Datenschutzbehörde muss eine erste Rechtmäßigkeitsprüfung vornehmen können

Die Informationspflicht

- Art 13 (1): Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:
  - Kontaktinformationen
  - Rechtsgrundlage der Verarbeitung
  - Berechtigte Interessen
  - Empfänger, Dauer
  - Beschwerderecht, etc…

Die Informationspflicht

- Art 14 (1): Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:
  - Kontaktinformationen
  - Rechtsgrundlage der Verarbeitung
  - Berechtigte Interessen
  - Empfänger, Dauer
  - Beschwerderecht
  - Die Quelle der Daten, etc…

Die Informationspflicht

- Art der Informationspflicht:
  - Kein Medienbruch
  - Verweis auf Website zulässig (?)
  - Aktive Unterrichtung!

E-Mail Marketing

- Voraussetzungen für den Newsletterversand / Direktwerbung
  - Einwilligung

ODER

  - Berechtigtes Interesse

  - Achtung: § 107 TKG

Meldepflicht

- Meldepflicht gegenüber der Behörde (Art 33 DSGVO)
  - Bei Verletzung des Schutzes personenbezogener Daten
  - Binnen 72 Stunden
    - außer die Verletzung führt zu keinem Risiko für die Rechte und Freiheiten der Betroffenen
    - die Meldung muss beinhalten: Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen

Meldepflicht

- Meldepflicht gegenüber dem Betroffenen
  - **Nicht**: bei verschlüsselten Daten
  - **Nicht**: bei hohem Aufwand

    (stattdessen: öffentliche Bekanntmachung)

Löschpflicht

- Grundsatz:

Die Verarbeitung personenbezogener Daten muss beendet werden, wenn diese für den Zweck der Verarbeitung nicht mehr notwendig sind.

- Anonymisierung
- Regelmäßige Überprüfung
- Offene Frage: Backup?

Betroffenenrechte

- Auskunft
  - Binnen eines Monats
  - Kostenlos

- Richtigstellung
- Löschung

- Prozessdefinition!

Datenschutzfolgeabschätzung

- Verpflichtend wenn riskante Datenanwendung
- Liste der Behörde

- Umfangreiche Dokumentationspflichten der Risiken, der Verarbeitungsvorgänge, der Folgen, der Notwendigkeit der Verarbeitung, etc…

Datenschutzbeauftragter

- „Berufliche Qualifikation
  - Laufende Fortbildung
- Intern oder extern
- Veröffentlichung der Kontaktdaten
- Ressourcen Bereitstellung
- Abberufungs- und Benachteilungsschutz
- Überwachung und Beratung

Minimalumsetzung

- Verzeichnis der Verarbeitungstätigkeiten
- Auftragsverarbeiterverträge
- Informationspflicht
- Mitarbeiterschulung
- Technische und organisatorische Maßnahmen

DSGVO

- Sanktion:
  - „wirksam, verhältnismäßig und abschreckend“
- Geldbuße:
  - bis zu EUR 10 Mio (oder 2% des weltweiten Jahresumsatzes)
  - bis zu EUR 20 Mio (oder 4% des weltweiten Jahresumsatzes)
  - zuständig: Aufsichtsbehörde

Danke für die Aufmerksamkeit

Höhne
In der Maur
& Partner

Rechtsanwälte

Markus Dörfler
E: markus.doerfler@h-i-p.at
T: 01/521 75-41
www.h-i-p.at
datenschutz-recht.at

Herzlichen DANK

UNTERLAGEN zur Veranstaltung

http://wko.at/stmk/rs-va

Weitere INFOS

http://wko.at/datenschutz

ANFRAGEN

E rechtsservice@wkstmk.at oder T 0316/601-601