Was ist wirklich neu an der DSGVO? Was muss man wirklich tun als Verantwortlicher?

MR Dr. Waltraut Kotschy

Informationsveranstaltung des Gemeindebundes Steiermark

zur EU Datenschutz-Grundverordnung

26. März 2018

Die neuen EU-Regelungen

- Die neue EU Datenschutz-Grundverordnung (DSGVO), 2016/679, wird am **25. Mai 2018** wirksam (in Kraft schon seit 25. Mai 2016)
  - Sie wird als EU-Verordnung in Österreich unmittelbar gelten

- Die neue Datenschutz-Richtlinie (EU) 2016/680, die Datenschutz bei der Verbrechensbekämpfung und -verfolgung (einschließlich Gefahrenabwehr für die öff. Sicherheit) durch die zuständigen Behörden regelt

Die österreichischen Regelungen zur Anpassung and die neuen EU-Regelungen

Betreffend die DSGVO:

- Das neue „DSG“, BGBl I Nr. 120/2017, das einige generelle Anpassungen der österr. Rechtsordnung an die DSGVO vornimmt
- Zusätzliche Anpassungsgesetze in einzelnen Ressortbereichen sind in Vorbereitung

Betreffend die neue DS-Richtlinie:

- Umsetzung im Wesentlichen durch das 3. Hauptstück des DSG

Änderungen der Terminologie

- Änderungen in Richtung dBDSG

  „Auftraggeber“ → „Verantwortlicher“

  „Dienstleister“ → „Auftragsverarbeiter“

  „Zustimmung“ → „Einwilligung“

  „übermitteln“ ---→ kein terminus technicus mehr

Rechtsgrundlagen

- **Die diesbezüglichen Regelungen bleiben im Wesentlichen gleich**

  Hoheitsverwaltung nutzt Daten auf der Grundlage von

  Art. 6 (1)(e) DSGVO = bisheriger Art. 7 (e) Datenschutz-Richtlinie

  → **keine weitreichenden Änderungen hinsichtlich der Zulässigkeit der Verwendung von personenbezogenen Daten (**Art. 6 (1) und Art. 9 DSGVO)

  → Was bisher in Österreich **zulässigerweise** verarbeitet wurde, darf mit 98,0% Wahrscheinlichkeit auch in Zukunft verarbeitet werden

  → z.B. die neuen Regelungen über eine gültige Einwilligung entsprechen der schon jetzt herrschenden Anschauung (siehe z.B. WP 187 der Art. 29 Gruppe)

Materienspezifisches Datenschutzrecht

- Viele Datenschutzbestimmungen sind in österr. Materiengesetzen enthalten
- DSGVO verdrängt prinzipiell nationales Datenschutzrecht
- Soweit sie die Verarbeitung von personenbezogenen Daten im Rahmen von **gesetzlich übertragenen Aufgaben im öffentlichen Interesse** betreffen, werden die **österreichischen Regelungen von der DSGVO jedoch nicht verdrängt** (Art. 6 (2) DSGVO) – allerdings müssen die österr. Regelungen im Einklang mit der DSGVO stehen

→ im Bereich der **Hoheitsverwaltung** bleibt materienspezifisches österr. Datenschutzrecht aufrecht, allerdings nur soweit abgestimmt mit der DSGVO

→ ressortspezifische Anpassungsgesetze des Bundes

→ Landesrechts-Anpassungsgesetze??

Die wesentlichsten Änderungen in der GVO

Der „Verantwortliche“ wird stärker in die Pflicht genommen als bisher:

- Er muss die Zulässigkeit seiner Datenverarbeitungen selbständiger einschätzen als bisher - es gibt kein Meldeverfahren mehr, in dem die Rechtmäßigkeit einer Datenverarbeitung von der Behörde vorsorglich beurteilt wird
- Folgen falscher Beurteilung wesentlich gravierender als bisher
  - → hohe Strafandrohungen: bis zu 20 Mill. € oder bis zu 4 % des weltweiten Gesamtjahresumsatzes
  - → Wird sich im öff. Bereich, wo keine Verwaltungsstrafen verhängt werden, in erhöhter Missbilligung der Öffentlichkeit für Datenschutzverletzungen niederschlagen

Geänderte „Randbedingungen“

- Neue Pflichten für den Verantwortlichen, z.B:
  - Dokumentation (Art. 30)
  - Risikofolgenabschätzung (Art. 35 f)
  - Datenschutzbeauftragten bestellen (Art. 37 ff)
  - neue Rechte der Betroffenen:
    - Recht auf Einschränkung der Verarbeitung (Art. 18)
    - Widerspruchsrecht (Art. 21)
- Verschärfung bestehender Pflichten, z.B.
  - Informationspflicht ausgeweitet (Art. 13/14)
  - Fristen zur Beantwortung von Begehren der Betroffenen auf 1 Monat verkürzt (Art. 12)
  - Meldung an Datenschutzbehörde bei Verletzungen der Datensicherheit (Art. 33 f)
  - ausführlichere Vereinbarungen mit Auftragsverarbeitern (Art. 28 f)
- Neue Möglichkeiten der Absicherung:
  - Zertifizierung (Art. 42 f)
  - genehmigte Codes of Conduct („Verhaltensregeln“, Art. 40 f)

Besondere Randbedingungen für den öff. Bereich? (1)

- DSGVO – Rechtsgrundlagen:

  eine „Behörde“ kann sich nicht auf bloße „berechtigte Interessen“ (Art. 6 (1) f DSGVO) stützen

- DSGVO – Pflichten des Verantwortlichen:

  „Behörden und öff. Stellen“ müssen einen Datenschutzbeauftragten bestellen

- DSGVO – Rechte des Betroffenen:

  Recht auf Datenübertragbarkeit gilt nicht gegenüber „Aufgaben, die im öff. Interesse liegen oder in Ausübung öff. Gewalt erfolgen“

- DSGVO – Zuständigkeit im Aufsichtsverfahren:

  zuständig ist immer nur die Aufsichtsbehörde am Sitz der „Behörde“ – keine grenzüberschreitenden Verfahren

Besondere Randbedingungen für den öff. Bereich? (2)

- **Abgrenzung öffentlicher – privater Bereich** in § 26 DSG:

  „Verantwortliche des öffentlichen und des privaten Bereichs“:

  entscheidend ist, so wie bisher im DSG 2000, die rechtliche Form der Einrichtung des Verantwortlichen

  z.B. als GmbH oder AG → priv. Bereich (außer bei Beleihung)
  als Körperschaft des öff. Rechts → öff. Bereich

- Wofür soll diese Abgrenzung gelten?

  für die erwähnten Fälle der DSGVO? Es existiert diesbez. keine Öffnungsklausel in der DSGVO für nationales Recht

  für die Bußgeldverhängung????

Besondere Randbedingungen für den öff. Bereich? (3)

- Art. 83 Abs. 7 DSGVO erlaubt es dem nationalen Gesetzgeber festzulegen, inwieweit **Bußgelder** gegen „Behörden und öffentliche Stellen“ verhängt werden können
- Abgrenzung der Möglichkeit, Bußgelder zu verhängen **in § 30 (5) DSG**:

  „(5) Gegen Behörden und öffentliche Stellen können keine Geldbußen verhängt werden.“

  → Abgrenzung materiell?

  dann wäre nur Hoheitsverwaltung ausgenommen

  → oder Abgrenzung formell?

  Form der Errichtung iSd § 26 DSG? Dann wäre auch Privatwirtschaftsverwaltung ausgenommen

„öffentliche Stelle“

- RICHTLINIE (EU) 2016/2102 über den barrierefreien Zugang zu Websites öffentlicher Stellen: Für die Zwecke dieser Richtlinie

  „bezeichnet der Ausdruck „öffentliche Stelle“ den Staat, die Gebietskörperschaften, die Einrichtungen des öffentlichen Rechts im Sinne der Definition in Artikel 2 Absatz 1 Nummer 4 der Richtlinie 2014/24/EU oder Verbände, die aus einer oder mehreren solcher Körperschaften oder Einrichtungen des öffentlichen Rechts bestehen, sofern diese Verbände zu dem besonderen Zweck gegründet wurden, im Allgemeininteresse liegende Aufgaben nicht gewerblicher Art zu erfüllen;“

  → keine Privatwirtschaftsverwaltung

RICHTLINIE 2014/24/EU über die öffentliche Auftragsvergabe bringt noch zusätzlich Finanzierung aus öff. Mitteln als Definitionselement ins Spiel und verlangt Rechtspersönlichkeit, (was aber bei der „öff. Stelle“ nach Datenschutzrecht sicherlich keine Rolle spielt)

Neuerungen im Detail

Dokumentation nach Art. 30 DSGVO

- An die Stelle der Meldung an das Datenverarbeitungsregister für neue Verarbeitungen tritt die Pflicht des Verantwortlichen, seine Verarbeitungen zu dokumentieren und die Dokumentation für die Aufsichtsbehörde bereit zu halten
- Inhalt der Dokumentation ist in Art. 30 festgelegt
- Was es ab 25. Mai nicht mehr geben wird, sind Standardanwendungen im Sinne der Standard- und Muster-Verordnung 2004

  → es müssen in Hinkunft **ALLE Verarbeitungen dokumentiert** werden, auch die bisherigen Standardverarbeitungen

Dokumentation der Rechtsgrundlagen?

- Art. 30 DSGVO verlangt – erstaunlicherweise – keine Aussage über die Rechtsgrundlagen einer Datenverarbeitung
- Wohl aber sind solche Aussagen notwendig bei der Information der Betroffenen nach Art. 13 und 14, sowie
- Bei der Auskunftserteilung nach Art. 15

→ man braucht eine zusätzliche Dokumentation, die aufzeigt, wie es mit den Rechtsgrundlagen der Datenverarbeitung im Detail steht

→ Datenverarbeitung ohne ausreichende Rechtsgrundlagen ist ein schwerer Verstoß: Verletzungen der Art. 6 und 9 DSGVO sind gem. Art. 83 Abs. 5 lit.a mit bis zu 20 Mill € zu bestrafen

Datenschutz-Folgenabschätzung

- Weitere zusätzliche Dokumentation notwendig:

  Der Verantwortliche muss schriftlich nachweisen können, dass er

  - die mit seiner Datenverarbeitung verbundenen Risiken geprüft hat und
  - Maßnahmen zur Risikoverminderung eingerichtet hat.

  Wenn trotz Maßnahmen ein „hohes Restrisiko“ bleibt, muss er die Datenschutzbehörde befassen zur Klärung, ob und unter welchen Bedingungen die Verarbeitung durchgeführt werden darf

  → Untersagung möglich!

Risikofolgenabschätzung – Fortsetzung:

- Verordnungen der Datenschutzbehörde fehlen noch:

  → „black list“: Datenverarbeitungen, bei welchen Risikoabschätzung jedenfalls durchgeführt werden muss und schriftlich vorgelegt werden kann

  → „white list“: Datenverarbeitungen, bei welchen Risikoabschätzung jedenfalls NICHT durchgeführt werden muss

- Der nationale Gesetzgeber kann im Bereich des Art. 6 (1) e (= Hoheitsverwaltung) oder Art. 6 (1) c (gesetzliche Verpflichtungen) aber bei Regelung der konkreten Verarbeitungsvorgänge eine allgemeine Risikofolgenabschätzung durchführen, womit sie der einzelnen Verantwortliche nicht nochmals durchführen muss

  → wie erkennbar, ob schon allgemein durchgeführt?

Der Datenschutzbeauftragte

- „Behörden und öffentliche Stellen“ müssen für ihre Datenverarbeitung einen Datenschutzbeauftragten bestellen
- Bestellung für mehrere Verantwortliche?
  „ unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe“ möglich
- Wer kann bestellt werden?
  - Auch „externe“ Datenschutzbeauftragte sind zulässig, d.h. Nicht-Mitarbeiter
  - Person muss berufliche Qualifikation und Fachwissen im Datenschutzbereich haben
  - Ein DSBeauftragter im öff. Bereich „ist bezüglich der Ausübung seiner Aufgaben weisungsfrei“ (§ 5 Abs. 3 DSG), aber berichtspflichtig hinsichtlich seiner Tätigkeit, „insoweit ….als dies nicht seiner Unabhängigkeit widerspricht“.
- Kontaktdaten des DSBeauftragten → Homepage des Verantwortlichen!

Aufgaben des Datenschutzbeauftragten

- Beratung „des Verantwortlichen“ (oder Auftragsverarbeiters) in Datenschutzfragen, d.h.

  - der Datenschutzbeauftragte muss Zugang haben zur Leitungsebene des Verantwortlichen (Auftragsverarbeiters), damit sein Rat „ankommt“

  - der Datenschutzbeauftragte muss Zugang in der ganzen Organisation des Verantwortlichen/Auftragsverarbeiters haben zu den relevanten Informationen, die er zur Beurteilung der Situation braucht

  → man muss organisatorische Vorkehrungen treffen

Neue Betroffenenrechte

- Information des Betroffenen = nunmehr „ein Recht“

  war bisher in Ö nur eine Pflicht des Auftraggebers, aber kein subj. Recht des Betroffenen

- Recht auf Einschränkung der Verarbeitung,
  - solange Richtigkeit oder Zulässigkeit der Datenverarbeitung strittig ist, oder
  - Keine Löschung, wenn der Betroffene Daten zu Beweiszwecken braucht
- [Recht auf Datenübertragbarkeit: gilt nicht gegenüber der Hoheitsverwaltung]
- Widerspruchsrecht:

  bei Datenverarbeitung aufgrund von Art. 6 (1) e;

  Rechtsfolge der Erhebung von Widerspruch → Beweislastregel: der Verantwortliche muss beweisen, dass er ein Verwendungsinteresse hat, das das Schutzinteresse des Betroffenen überwiegt

Ausweitungen von Pflichten

Die Informationsrechte der Betroffenen werden gestärkt:

→ sie sind umfangreicher als bisher

→ die generelle Ausnahme von der Informationspflicht zugunsten gesetzlich geregelter Datenverwendung gibt es nicht mehr : nur wenn Daten von Dritten ermittelt werden und nicht vom Betroffenen, befreit eine gesetzliche Regelung von der Pflicht zur Information

→ einzige generelle Ausnahme: „wenn der Betroffene die Information bereits hat“

→ „unverhältnismäßiger Aufwand“ oder „Unmöglichkeit“ befreien nur allenfalls bei Ermittlung von Dritten

Wann und wie ist zu informieren?

WANN?

- Bei der Datenermittlung beim Betroffenen
- Im Fall der Datenermittlung bei Dritten: spätestens innerhalb von 1 Monat ab Erlangung der Daten

WIE?

- Wenn man physisch oder virtuell mit dem Betroffenen kommuniziert, z.B:
  - auf der Webseite der Gemeinde
  - am Schalter
  - bei der Ausfüllung von Antragsformularen
- durch Zusenden von Information
- ……..??

Fristen

- Tendenz zur Verkürzung maßgeblicher Fristen gegenüber der bisherigen österr. Rechtlage:
  - Frist zur Beantwortung von Begehren von Betroffenen nicht mehr 8 Wochen, sondern nunmehr nur 1 Monat
  - kann allerdings um zwei weitere Monate ausgedehnt werden wegen Komplexität oder Anzahl von Anträgen (eines Betroffenen)

    setzt voraus, dass dies dem Betroffenen innerhalb der

    1- Monats-Frist mitgeteilt wird

Meldung von Verletzungen der Datensicherheit

- Wenn Daten verloren gehen, zerstört werden, von Unbefugten erlangt werden etc. und es nicht wahrscheinlich ist, dass aus der Verletzung kein Risiko für die Betroffenen entsteht

  → Meldung an die Datenschutzbehörde, möglichst binnen 72 Stunden

- Wenn voraussichtlich ein hohes Risiko für die Betroffenen aus der Verletzung folgt

  → zusätzlich Benachrichtigung der Betroffenen

  → Ausnahmen: wenn verlorene Daten z.B. verschlüsselt waren

  nachträglich effektive Schutzmaßnahmen getroffen wurden

  unverhältnismäßiger Aufwand → öff. Bekanntmachung

Vereinbarungen mit Auftragsverarbeitern

- Art. 28 DSGVO enthält umfangreiche Regelung darüber, welche Verpflichtungen der Auftragsverarbeiter gegenüber dem Verantwortlichen eingehen muss
- Die bestehenden Mustervereinbarungen reichen nicht mehr aus

  → Die Datenschutzbehörden und auch die EU-Kommission können neue Standardvertragsklauseln festlegen

  → derzeit noch nicht erlassen

  → wie kann Übergangszeit mit vertretbarem Aufwand überbrückt werden?

Vereinbarungen mit anderen Verantwortlichen - Informationsverbundsysteme

- Es gibt keine äquivalente Bestimmung in der DSGVO zu § 50 DSG 2000
- Am ehesten kommt Art. 26 über die gemeinsam Verantwortlichen dem nahe
  - eigene Verträge notwendig, die vor allem die Reaktion auf die Ausübung der Betroffenenrechte regeln müssen
  - Wenn Informationsverbundsysteme gesetzlich vorgesehen sind, wie z.B. das Zentrale Melderegister, müsste in Zukunft gesetzlich für dieses System konkret das festgelegt werden, was generell von Art. 26 DSGVO verlangt wird:

    v.a. wer vertritt die gemeinsame Datenverarbeitung nach außen, gegenüber den Betroffenen?

Verhaltensregeln und Zertifizierung

- Codes of conduct müssten wichtiger werden als bisher, da sie eigentlich die einzige zugelassene Art der Formulierung von materienspezifischem Datenschutzrecht *im privaten Bereich* sind

  - für die Gemeinden allenfalls in privatwirtschaftlichen Bereich interessant

  - Befolgung kann besonderen Milderungsgrund bei der Verhängung von Geldbußen darstellen

- Zertifizierung: denselben Milderungseffekt hat die Einhaltung eines zertifizierten Verfahrens

Rechtszug

- § 26 DSG:

  „ (2) Verantwortliche des öffentlichen Bereichs sind Partei in Verfahren vor der Datenschutzbehörde.

  (3) Verantwortliche des öffentlichen Bereichs können Beschwerde an das Bundesverwaltungsgericht und Revision beim Verwaltungsgerichtshof erheben.“

- Abgrenzung in diesem Fall eindeutig nach formalen Kriterien, nämlich der Einrichtung in Formen des öff. oder des privaten Rechts

Fazit

- Was muss vor allem bis zum 25. Mai getan werden?
  - Dokumentation für alle Datenverarbeitungen
  - Bestellung eines Datenschutzbeauftragten
  - Überprüfung der Erfüllung der Informationspflicht
  - Ergänzung der Verträge mit den Dienstleistern („Auftragsverarbeitern“)

Danke für Ihre Aufmerksamkeit!