Aktuelle Entwicklungen im Datenschutzrecht

Dr. Eva Souhrada-Kirchmayer

23. Mai 2012

7. Österreichischer IT-Rechtstag

Entwurf einer DSG-Novelle 2012
397/ME BlgNR 24. GP *(derzeit „auf Eis“)*

DATENSCHUTZBEAUFTRAGTER

- Kann auf **freiwilliger Basis** bestellt werden
- Mindestbestellungsdauer 3 Jahre
- **Fachkunde, Zuverlässigkeit** gefordert
- Meldung der Bestellung an die DSK, öffentliche Liste der DSB im Internet Ist in dieser Funktion weisungsfrei
- Überwachung der Einhaltung des DSG 2000 beim Auftraggeber; Hinwirkung auf Herstellung des rechtmäßigen Zustands, Möglichkeit einer Eingabe an die DSK
- Führung eines **Verzeichnisses der Datenanwendungen** des Auftraggebers (Einsicht für betroffene Personen)

Neuordnung der Vorabkontrolle

VORABKONTROLLPFLICHTIG sind Datenanwendungen, wenn sie

1. **sensible** Daten enthalten
2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die **Persönlichkeit** des Betroffenen einschließlich seiner **Fähigkeiten**, seiner **Leistung**, seiner **wirtschaftlichen Lage** oder seines **Verhaltens** zu bewerten.

Neuordnung der Vorabkontrolle *(Fortsetzung)*

NICHT mehr vorabkontrollpflichtig sind

- **Informationsverbundsysteme**
- Datenanwendungen, die **strafrechtlich relevante Daten** enthalten
- **Videoüberwachungen**
- Datenanwendungen, die sich auf die **ausdrückliche Zustimmung des Betroffenen** gründen und
- Datenanwendungen, die sich auf datenschutzrechtlich genügend **determinierte Gesetze oder Verordnungen** gründen (nachdem allfällige Stellungnahme der DSK berücksichtigt wurde

DSG-Novelle 2012 – Weitere Punkte

- DSK kann Rechtshilfeersuchen an die **Bezirksverwaltungsbehörden** oder die **Landespolizeidirektionen stellen,** denen Folge zu leisten ist
- Befassung der DSK **vor Erlassung von Gesetzen**, die **wesentliche Fragen des Datenschutzes unmittelbar betreffen**
- Erweiterung der Strafbestimmungen

Übergangsbestimmungen

- Registrierung von „alten" Meldungen (vor DVR-Online), **die nicht der Vorabkontrolle unterliegen**
- Wenn Verbesserungsantrag seit drei Jahren nicht Folge geleistet wurde – als Zurückziehung gewertet
- Wenn Meldepflicht im Nachhinein weggefallen ist – als Zurückziehung gewertet
- Wenn nicht mehr vorabkontrollpflichtig – nur mehr meldepflichtig.

EuGH-Urteil vom 16. 10. 2012
Vertragsverletzungsverfahren C-614/10

Verurteilung der Republik Österreich.

DSK **ist nicht völlig unabhängig**, und zwar aus folgenden Gründen:

- geschäftsführendes Mitglied ist „Bundesbeamter“(Beamter des Bundeskanzleramtes) und daher indirekt vom Bundeskanzleramt abhängig
- organisatorische Eingliederung der Geschäftsstelle der DSK ins Bundeskanzleramt
- uneingeschränktes Unterrichtungsrecht des Bundeskanzlers gegenüber der Datenschutzkommission

DSG-Novelle 2013 (BGBl I Nr. 17/2013)

- In Kraft getreten am 1. Mai 2013
- Datenschutzkommission ist nunmehr eine **eigene Dienstbehörde** und **Personalstelle** (im „Ressortbereich Bundeskanzleramt“)
- **Eingeschränktes Unterrichtungsrecht** des Bundeskanzlers (besteht nur, soweit dies nicht der Unabhängigkeit widerspricht)
- Übernahme der Bediensteten der Geschäftsstelle im Bundeskanzleramt als „Bedienstete der Datenschutzkommission“
- Weisungsgebundenheit gegenüber dem **Vorsitzenden** (dieser hat die Dienstaufsicht und die Weisungsbefugnisse weitgehend an das geschäftsführende Mitglied delegiert – Änderung der GO der DSK)

Entwicklungen in der EU

- Vorschlag für eine Datenschutz-Grundverordnung KOM(2012) 11 endgültig
- Vorschlag für eine Richtlinie für den Bereich Polizei und Justiz (Strafsachen) KOM(2012) 10 endgültig

→ Verhandlungen in RAG DAPIX und LIBE-Ausschuss des EP

VO-Vorschlag

- Einerseits Reduktion der Verwaltungslasten (Abschaffung der generellen Meldepflicht)
- Aber: mehr (sichtbare Verantwortung für den Auftraggeber – so genanntes „accountability principle“)

VO-Vorschlag *(Fortsetzung)*

Accountability Principle:

- Privacy by design privacy by default
- Datenschutzbeauftragter (weit gehende Ausnahmen)
- Dokumentationspflichten (weit gehende Ausnahmen)
- Datenschutzfolgeabschätzungen bei riskanten Datenanwendungen
- Vorherige Zurateziehung der Datenschutzbehörde

VO-Vorschlag *(Fortsetzung)*

Stärkung der Betroffenenrechte, insbesondere in der „online-Umgebung“

- Ausdrückliche Zustimmung
- „Right to be forgotten“ – detailliertes Löschungsrecht
- Recht auf Datenportabilität

VO-Vorschlag *(Fortsetzung)*

Stärkung der Datenschutzbehörden

- einheitliche Befugnisse, z. B. auch Anordnungsbefugnis in allen Bereichen, Strafbefugnisse, „Awareness raising“
- Regelungen für die Zusammenarbeit der Aufsichtsbehörden unter Einbeziehung des „Europäischen Datenschutzausschusses“, Zuständigkeitsregelung: „one stop shop“

VO-Vorschlag *(Fortsetzung)*

- Neuregelungen zum Transfer von Daten in Drittstaaten (weiterhin Transfer in Staaten mit einem angemessenen Datenschutzniveau, genaue Regelung der „Binding Corporate Rules“, weit gehende Ausnahmen)
- Strafen / Strafhöhe

RL-Vorschlag

- Gilt für Behörden im Bereich „Polizei und Justiz“
- Bleibt im Datenschutzniveau deutlich hinter dem VO-Vorschlag zurück
- Bleibt in einigen Punkten sogar hinter dem Rahmenbeschluss 2008/977/JI zurück (kritisch zu sehen sind vor allem die Bestimmungen punkto Zweckbindung, Datentransfer in Drittstaaten und an internationale Organisationen, fehlende Ausgestaltung des accountability principles, mangelnde Befugnisse der Aufsichtsbehörden)
- Gilt im Gegensatz zum Rahmenbeschluss auch für den innerstaatlichen Bereich

VO-Vorschlag – einige offene Punkte

- Anwendungsbereich
- „Household exemption“
- Frage der (ausdrücklichen) Zustimmung
- „risk-based approach“
- optionaler Datenschutzbeauftragter?
- pseudonymisierte Daten
- Verhältnis Datenschutz und freie Meinungsäußerung, Zugang zu öffentlichen Dokumenten
- Verhaltensregeln und Zertifizierung
- Mehr Flexibilität im öffentlichen Bereich?
- Kompetenzen der Datenschutzbehörden (one stop shop als „single contact point“?)

Weitere Vorgangweise

- Europäisches Parlament: ca. 3500 Änderungsvorschläge, Positionierung für Juli d. J. erwartet
- DAPIX-Gruppe: dritte Lesung der VO beendet – Befassung von COREPER und JI-Rat mit wichtigen Fragen (Juni 2013)
- EP: Vor der parlamentarischen Sommerpause 2013: Orientierungsabstimmung im LIBE-Ausschuss, ab Herbst 2013 (je nach Verhandlungsstand im Rat) Verhandlungsbeginn zwischen EP, Rat und Europäischer Kommission ("Trilog")
- RL – Stagnation – ist Junktimierung VO mit RL durch EP noch aufrecht? (ca. 700 Änderungsvorschläge)

ELGA
Gesundheitsdiensteanbieter bisher

- Krankengeschichte der PatientInnen
- kann auch automationsunterstützt geführt werden

ELGA

Informations(verbund)systeme

Datenfluss zwischen mehreren Auftraggebern (GDA)

→ Lese- bzw. Eintragungsbefugnis (nach Rollen abgestuft)

Arbeitspapier „Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)“ (WP 131) der Art. 29-Gruppe

- Es gilt die RL 95/46/EG, wie etwa die **allgemeinen Grundsätze** (Art. 6 DSRL, z.B. Zweckbindung, Grundsatz der Datenqualität, begrenzte Speicherung etc.), die **Informationspflichten** (Art. 10), **Auskunfts-, Richtigstellungs- und Löschungsrecht** (Art. 12), **Datensicherheit** (Art. 17)
- Art. 8 (sensible Daten) – Abs. 4: Die Mitgliedstaaten können vorbehaltlich angemessener Garantien aus Gründen eines wichtigen öffentlichen Interesses entweder im Wege einer nationalen Rechtsvorschrift oder im Wege einer Entscheidung der Kontrollstelle andere als die in Absatz 2 genannten Ausnahmen vorsehen.

Überlegungen zu einem geeigneten Rechtsrahmen für EPA-Systeme

- Wahrung des **Selbstbestimmungsrechts** (opt-in, opt-out)
- PatientInnen sollen die Möglichkeit haben, die Weitergabe an andere GDA zu verhindern
- **Kompletter Ausstieg** muss möglich sein
- **Identifizierung und Authentifizierung** von Patienten und medizinischem Personal
- Modulare Zugangsrechte zu EPA-Systemen, z.T. opt-in
- Besondere Zugangskontrollen unter Mitwirkung des Patienten („versiegelte Umschläge“)
- Direkter elektronischer Zugriff der PatientInnen auf ihre EPA

Überlegungen zu einem geeigneten Rechtsrahmen für EPA-Systeme *(Fortsetzung)*

- Keine Verwendung der EPA für andere Zwecke (Vertrauen ins System!)
- **Organisationsstruktur eines EPA-Systems** (dezentrale Speicherung? zentrale Speicherung?)
- Datenkategorien – „erhebliche“ Information
- Kein Transfer in Drittstaaten
- **Datensicherheit** (Zugriff durch Unbefugte faktisch unmöglich) sein
- Besonders hohe Transparenz notwendig
- Haftung
- Kontrollmechanismen für die Verarbeitung von Daten (besonderes Schiedsverfahren)

ELGA-G

- setzt in wesentlichen Teilen Papier der Art. 29-Gruppe um
  - **Online-Einsicht** in eigene Daten und darüber, wer was abgefragt und eingetragen hat (§ 16 Abs. 1)
  - Auskunftsrecht nach dem DSG 2000
  - **Aushänge** in den Räumen der GDA (§ 16 Abs. 4)
  - **Informationspflicht des BMG** nach §16 Abs. 5 – allgemein Transparenz über die Betroffenenrechte
  - **Jährliche Aufklärung** durch die Sozialversicherung (Art. 2 bis 5 ELGA-G) über Betroffenenrechte

ELGA-G *(Fortsetzung)*

- Kompletter **Ausstieg** ist möglich
- **Widerspruch** im Einzelfall möglich („ELGA ist ein löchriger Käse“)
- Identifizierung und Authentifizierung von Patienten und GDA
- Abstufung der Berechtigungen
- Dezentrale/zentrale Speicherung
- Datensicherheitsmaßnahmen
- ELGA-Ombudsstelle
- Datenkategorien: ELGA-Gesundheitsdaten sind in § 2 Z 9 näher umschrieben.
- Sanktionen

Probleme

Frage der **optimalen PatientInnenautonomie**:

Durchgängiges Opt-out Modell (keine zustimmungsbedürftigen Speicherungen)

- Opt-out bezüglich genereller Teilnahme
- Opt-out im Einzelfall

⇒Gelinderes Mittel der Zustimmung?

⇒Woher weiß der Patient, dass im konkreten Fall seine Daten für ELGA verwendet werden?

Probleme *(Fortsetzung)*

Unklarheiten (z.B. beim Widerspruchsrecht)

- „Im Zuge der Ermittlung der Identitätsdaten mittels e-card-System…ist **im selben Arbeitsschritt, aber technisch von den Datenflüssen des ELSY…getrennt**, auch ein **allfälliger Widerspruch** zu dokumentieren."

  → Ordinationshilfe? Info der PatientInnen?

- Über das Widerspruchsrecht ist der ELGA-Teilnehmer/die ELGA-Teilnehmerin **insbesondere** bei ELGA-Daten, die sich auf HIV-Infektionen, psychische Erkrankungen, Daten gemäß § 71a Abs. 1 GTG oder Schwangerschaftsabbrüche zu informieren.

  → Wer informiert worüber?

Probleme *(Fortsetzung)*

- „ELGA-Gesundheitsdiensteanbieter sind gegenüber ELGA-Teilnehmer/innen nicht zur Nachfrage über die Ausübung von TeilnehmerInnenrechten verpflichtet“ → heißt das, das GDA das Recht haben, nach Ausblendungen zu fragen?
- Frage des **Vertrauensverhältnisses** zwischen GDA und PatientIn
- Gefahr des latenten Unterdrucksetzens/sich unter Druck Fühlens/ der latenten Diskriminierung
- Verwendungsbeschränkung nicht in Verfassungsrang geregelt
- Wo Daten anfallen, besteht die Gefahr des Datenmissbrauchs (es gibt keine absolute Datensicherheit; Gefahr des Missbrauchs durch legitime Abfrager?)

RL 2006/24/EG („Vorratsdatenspeicherungs-RL“)

- Stellt formell eine Änderung der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) dar.

Vorratsdatenspeicherungs-RL *(Fortsetzung)*

- Verpflichtet Provider dazu, dass bestimmte Telekommunikationsdatenkategorien, die von Anbietern öffentlich zugänglicher Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, auf Vorrat gespeichert werden → keine Inhaltsdaten
- RL regelt nur **Speicherung** (gibt einen Rahmen von sechs Monaten bis zu zwei Jahren vor)
- Zweck: Diese Daten sollen zum Zwecke der Ermittlung, Feststellung und Verfolgung von **schweren Straftaten** zur Verfügung stehen

Neuere Entwicklungen und Probleme

- Verhältnismäßigkeit der RL? Inzwischen Evaluierungsbericht der Europäischen Kommission
- Verhältnismäßigkeit der Umsetzung in den MS?
- Umsetzung in AT: Beschluss einer TKG-Novelle (BGBl I Nr 27/2011), ergänzend dazu StPO- und SPG-Novelle (BGBl I Nr 33/2011), Entschärfung durch Abänderungsanträge und Entschließungen
- Speicherung und Abfragen für SPG-Zwecke und Strafverfolgung leichter Straftaten ist keine Umsetzung der Vorratsdatenspeicherungs-RL → Art. 15 ePrivacy-RL

Aktuelles zur Vorratsdatenspeicherung

- Änderung der Vorratsdatenspeicherungs-RL?
- Irisches Verfahren beim EuGH
- Österreichische Bürgerinitiative „Stoppt die Vorratsdatenspeicherung“ (auch Hearing dazu im Justizausschuss)
- Vorlage des österreichischen VfGH beim EuGH
- Vorlage der DSK beim EuGH

Vorlage des VfGH an den EuGH
(28. November 2012) Rs. C-594/12

- Verhältnis der Rechtsinstrumente im Datenschutz (RL 95/46/EG bzw. VO 45/2001/EG) zu Art. 8 Grundrechte-Charta? Verhältnis des Sekundärrechts zu den in Art. 8 Abs. 2 bzw. Art. 52 Abs. 1 und 3 enthaltenen Schranken?
- Zur Frage der „Wahrung höherer Schutzniveaus“ – geht ein höheres Schutzniveau (etwa in § 1 DSG 2000) den Schranken vor, die sich aus der Grundrechte-Charta selbst ergeben?
- Bedeutung der Rechtsprechung des EGMR für Auslegung des Art. 8 Grundrechte-Charta?

Vorlage der DSK an den EuGH

(18. Jänner 2013) Rs. C-46/13

1. Sind Bestimmungen der Richtlinie zur Vorratsdatenspeicherung so auszulegen, dass die Betroffenen nicht zum Kreis der „besonders ermächtigten Personen“ zählen und ihnen somit kein Auskunftsrecht gegenüber Telekommunikationsunternehmen zusteht?

2. Sind die Bestimmungen der Datenschutzrichtlinie im Licht der Vorratsdatenspeicherungsrichtlinie derart auszulegen, dass das Recht auf Auskunft gegenüber einem Telekommunikationsunternehmen beschränkt oder ausgeschlossen werden kann?

3. Falls Frage eins bejaht wird, ist die Beschränkung des Auskunftsrechts in Bezug auf Vorratsdaten mit der Grundrechtecharta vereinbar und somit gültig?

Danke für Ihre Aufmerksamkeit!

Dr. Eva Souhrada-Kirchmayer
Datenschutzkommission
www.dsk.gv.at
+43 1 53115/202525