Rechtliche Herausforderungen / Rahmenbedingungen

Wesentliche Neuerungen im EU-Datenschutzrecht

Gérard LOMMEL, Regierungskommissar für Datenschutz bei der staatlichen Verwaltung
Staatsministerium Luxemburg

Quellen des europäischen Datenschutzrechts

- **Artikel 8** der **Europäischen Menschenrechtskonvention** (4. 11.1950 in Rom unterzeichnet) und Rechtssprechung des Europäische Gerichtshof für Menschenrechte (EGMR)
- 1970er Jahre: Erste Datenschutzgesetze und Empfehlungen des Europarats (1973-74)
- Straßburg, 28/01/1981**: Europarats-Übereinkommen** Nr.108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten
- **RICHTLINIE 95/46/EG** des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personen-bezogener Daten und zum freien Datenverkehr

Reform des EU Datenschutz-Rechtsrahmen

- **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 **(E-Privacy)**
- **Rahmenbeschluss 2008/977/JAI** des Rates vom 27. 11. 2008 über den Schutz personenbezogener Daten, die im Rahmen der **polizeilichen und justiziellen Zusammenarbeit in Strafsachen** verarbeitet werden
- CHARTA DER GRUNDRECHTE DER EUROPÄISCHEN UNION (2010/C 83/02) und Rechtssprechung des EuGH
- 25. Januar 2012: Reformvorschlag der EU Kommission
- **4. Mai 2016:** Grundverordnung + Richtlinie im Amtsblatt veröffentlicht (anwendbar ab Mai 2018)

EU-DSGV: Wichtigste Neuerungen

- **Europaweit einheitliche Regeln** : kein Patchwork mehr ! Jedoch lässt die EU Datenschutzgrundverordnung beschränkt nationale Eigenausgestaltung (hoheitliche Aktivitäten des Staats) und Sonderregelungen (*Beschäftigtendatenschutz, Forschung*) zu; Eine separate EU Richtlinie für den Bereich des Strafrechts
- Das **«*Accountability*» -** Prinzip («*controllers + processors*»)
- Mehr **Transparenz, Stärkung der** Betroffenen**rechte**, auch online
- Bessere **Durchsetzungsfähigkeit: via** Beschwerden bei **DPAs** (Sofortmassnahmen/Bussgelder)und **wirksame** gerichtliche **Rechtsbehelfe** (Unterlassung, Löschung, Schadenersatz)
- Weniger admin. Aufwand; internationale Abstimmung zwischen Datenschutzbehörden: **One stop shop** und Kohärenzverfahren

« *Be able to demonstrate compliance* »

- Neue ***Accountability*** Anforderungen an alle Akteure: *Compliance*-Nachweis und Schutzmassnahmen :
- **Proaktive Risiko-/Folgenabschätzung und kontinuierliche Überprüfung** der Rechtmässigkeit , Zweckbeschränkung und Verhältnissmässigkeit der Datensammlung, -nutzung, -speicherung und-weitergabe
- « ***Data Protection by design & by default*** , D-P Policy »

  (abhängig von Art, Umfang, Umständen und Zwecken der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere des Risikos für Betroffene)
- « **Safeguards** »: technische Vorkehrungen und angemessene organisatorische Massnahmen, z.B. Pseudonymisierung und Verschlüsselung der Daten; Sensibilisierung der Mitarbeiter

Gestärkte individuellen Rechte und Freiheiten

- **Mehr Transparenz**: erweiterte Informationspflichten, « *Notice& choice* »: Spezielle Regeln bei Kindern
- **Einwilligung** gilt nur falls freiwillig, aktiv und eindeutig
- neues **Recht auf Vergessenwerden, Datenportabilität**
- **Auskunftrecht**, Zugang zu eigenen Daten, Recht auf **Berichtigung, Löschung**, bei widerrufener Einwilligung, Unrechtmässigkeit… (**« Widerspruchsrecht» nur in bestimmten Fällen** (z.B. Marketing; nicht falls Datenverarbeitung lebenswichtig oder per Gesetz oder Vertrag vorgesehen)
- Recht sich automatisierter **Profilkategorisierung** und maschienengestützter **Bewertung (Scoring)** zu entziehen

Neuer Fokus auf die Datensicherheit

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- **Angemessener Sicherheitsvorkehrungen sind Pflicht:** Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste müssen sichergestellt sein; granulare Rechteverwaltung Zugriffskontrolle und rasche operative Wiederherstellung bei Angriff oder technischem Zwischenfall
- Verweis auf «*state of the art* «*scalability*» & *standards*»
- Verfahren zur regelmässigen Überprüfung, Bewertung der Massnahmen und Evaluierung deren Wirksamkeit
- **Datenmissbräuche und Sicherheitsverletzungen** müssen Aufsichtsbehörden gemeldet werden (auch Benachrichtigung der betroffenen Personen Vorschrift, falls ein hohes Risiko für die Rechte und Freiheiten wahrscheinlich ist) *«Data Breach» = weit gefasst – unberechtigter Zugang genügt*

California Data Breach Report 2016 (2012-15)

- Malware und Hacking (unerlaubtes Eindringen in IT-System) 54% der Fälle, 90% der betroffenen Datensätze
- Verlust oder Diebstahl (physisch) : 22% der Fälle, 6% der betroffenen Datensätze
- Fehler von Mitarbeitern (Falscher E-Mail-Empfänger oder unbeabsichtigte Veröffentlichung auf Website) : 17% der Fälle, 4% der betroffenen Datensätze
- Missbrauch bzw. unautorisierte Nutzung von Zugangsrechten (intern) : 7% der Fälle, <1% der betroffenen Datensätze

Betriebliche Datenschutzbeauftragte als Berater des Managements & in-house Prüfer

- Bestellung von **Datenschutzbeauftragten** wird Pflicht im öffentlichen Bereich und bei privat-rechtlichen Betrieben die massiv sensible Daten verarbeiten oder systematisch *Profiling/monitoring* einsetzen *(Art. 37-39)*
- Einbindung in alle Datenschutzfragen, Zugang zu allen Verarbeitungsvorgängen, allen Managementebenen und den IT-Sicherheits-beauftragten, *CISOs, RSI/RSSI*
- Anlaufstelle für Aufsichtsbehörden und Reklamationen
- Stärkung der **Selbstregulierung** durch Zertifizierung oder freiwillige *Branchen*-Verhaltensregeln, (von den Daten-schutzbehörden geprüft, Einhaltung extern überwacht)

Vielen Dank für Ihre Aufmerksamkeit

gerard.lommel@me.etat.lu