Informationstag "Elektronische Signatur"

Gemeinsame Veranstaltung von TeleTrusT und VOI

Berlin, 17.09.2015

Die neue EU-Datenschutzverordnung und ihre Auswirkungen auf Verschlüsselung und Signatur

Ulrich Emmert
Partner esb Rechtsanwälte
Vorstand Reviscan AG
Stv. Vorstandsvorsitzender VOI e.V

Ulrich Emmert

Rechtsanwalt
Partner esb Rechtsanwälte
Lehrbeauftragter für
Wettbewerbs-, Urheber-
und Onlinerecht an der
Hochschule für Wirtschaft
und Umwelt in Nürtingen
Geschäftsführer einer
Unternehmensberatung
Vorstand des VOI e.V.

Informationssicherheit
Security Policies
Datenschutz
E-Mail-Archivierung
Haftungsrecht / AGB
Lizenzverträge
M&A
Kapitalgesellschaftsrecht
Umwandlungsrecht

esb Rechtsanwälte PartG
Schockenriedstr. 8A
70565 Stuttgart
Tel. 0711/469058-0
Fax 0711/469058-99
ulrich.emmert@kanzlei.de

www.kanzlei.de
www.reviscan.de
www.voi.de

Datenschutz

Abhören im Ausland

Entstehung der Verordnung

- Mitteilung der EU-Kommission vom 4. November 2010
- Öffentliche Anhörung
- Präsentation des Vorschlags der EU-Kommission für neuen Rechtsrahmen am 25. Januar 2012
- http://www.eu-datenschutzverordnung.de/downloads/entwurf-eu-datenschutzverordnung-2012.pdf
- Zwei neue Rechtsakte für den Datenschutz:
  - Datenschutz-Grundverordnung
  - Richtlinie für Justiz und Inneres

Letzte Entwurfsfassungen

- Konsolidierte Fassung der EU-Datenschutzverordnung vom 28.6.2014 http://www.computerundrecht.de/DS-GVO-konsolidiert.pdf
- Entwurfsfassung vom 19.12.2014 http://www.statewatch.org/news/2014/dec/eu-council-dp-reg-15395-14.pdf
- Neueste Entwurfsfassung Ministerrat http://www.computerundrecht.de/Verabschiedete_deutschsprachige_Fassung_der_allgemeinen_Ausrichtung_des_EU-Rats_zur_Datenschutz-GVO_v._11.06.2015.pdf

Synopse der Fassungen

- Vergleich der verschiedenen Fassungen durch den bayrischen Landesbeauftragten für den Datenschutz
- http://www.computerundrecht.de/BayLDA-Synopse_der_Datenschutz-GVO_v._24.06.2015.pdf

Verfahrensstände

- Entwurf Juni 2014 basiert im Wesentlichen auf der Fassung des Europäischen Parlaments vom März 2014
- Entwurf Dezember 2014 ist eine unbeabsichtigte Veröffentlichung aus den Verhandlungen des Ministerrats mit erheblicher Verwässerung des Entwurfs, teilweise sogar Verschlechterung gegenüber der Richtlinie
- Juni 2015 Entwurf der lettischen Ratpräsidentschaft nach Beratungen MInisterrat
- Deutschland trägt maßgeblich zur Verwässerung bei

Weiteres Verfahren

- Seit Einigung des Ministerrats auf Textvorschlag 3.6.2015 Beginn des sogenannten Trilogs zwischen Kommission, Parlament und Ministerrat
- Verabschiedung der Richtlinie durch Europäischen Rat
- Veröffentlichung im Amtsblatt der EU
- Einräumung einer Übergangsfrist bis von 2 Jahren zum endgültigen Inkrafttreten (Art. 91)

Anwendungsbereich

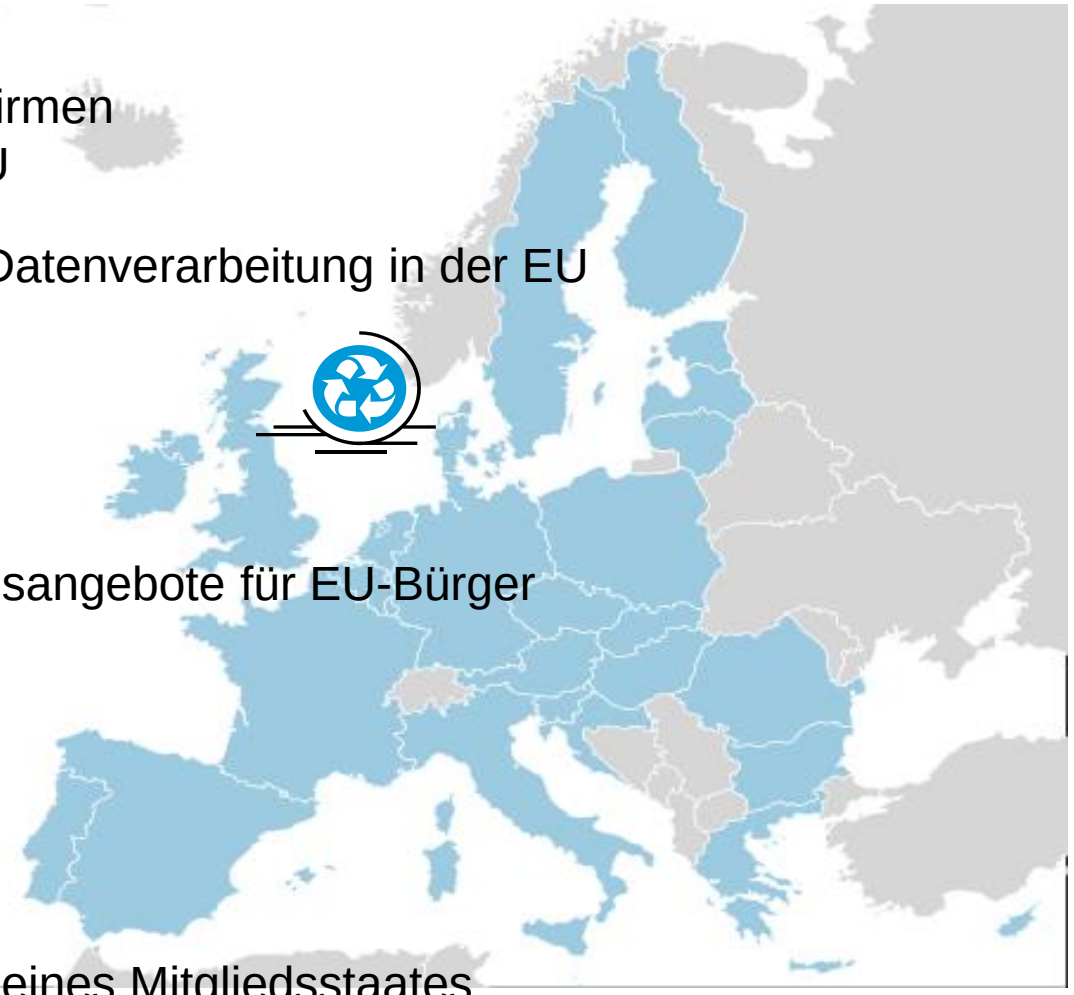
Auslandsniederlassungen von EU-Firmen
Auch bei Verarbeitung außerhalb EU

→ Datenverarbeitung in der EU

Waren- und Dienstleistungsangebote für EU-Bürger

→

Monitoring
von EU-Bürgern



Verarbeitung nach Recht eines Mitgliedsstaates

Ausnahmen

- Tätigkeit, die nicht dem Unionsrecht unterliegt
- Durch EU-Institutionen
- Durch Mitgliedsstaaten im Bereich der Außen- und Sicherheitspolitik
- Von einer natürlichen Person zu ausschließlich persönlichen oder familiären Zwecken
  - Gilt auch bei Veröffentlichung mit begrenztem Zugang
- Verhütung Aufdeckung Verfolgung von Straftaten

Sensible Daten Art. 9

Verarbeitung folgender Daten ist untersagt: (ausgenommen explizite Ausnahmen)

Gesundheit

Rasse oder ethnische Herkunft

Politische Überzeugungen

Sexualleben

Religions- oder Glaubens-zugehörigkeit

Genetische Eigenschaften

Strafurteile oder damit zusammen-hängende Sicherungsmaßregeln

Zugehörigkeit zu einer Gewerkschaft

Ziele Datenschutzkonzept

- Prüfung Vollständigkeit der Daten
- Prüfung Vollständigkeit, Vertraulichkeit, Verfügbarkeit, Belastbarkeit der Systeme auf Dauer
- Rasche Wiederherstellung der Daten bei Vorfällen unter Berücksichtigung dieser Ziele
- Zusätzliche Sicherheitsmaßnahmen bei sensiblen Daten mit IDS/CERT
- Prüfung / Evaluierung Sicherheitsmaßnahmen

Datenschutzkonzept Art. 22

- Einhaltung der Verordnung durch technische und organisatorische Strategien nachzuweisen
- Möglichkeit des Nachweises durch Zertifizierung oder Binding Corporate Rules

Datenschutz durch Technik Art. 23

- Pflicht zur Überprüfung der verwendeten technischen Mittel zum Schutz der Daten
- Prüfung des gesamten Lebenszyklus der Daten von der Entstehung bis zur Löschung
- Verfahrensgarantien zu
  - Richtigkeit
  - Vertraulichkeit
  - Vollständigkeit
  - Physische Sicherheit
  - Löschung

Datenschutz durch Technik Art. 23

- Berücksichtigung Folgeabschätzung
- Verantwortlichkeit von Verantwortlichem und Auftragsverarbeiter (neu)
- Nachweis Voraussetzung bei Ausschreibungen
- Datenminimierung und Ausschluss unbeschränkter Verbreitung soll sichergestellt werden

Mehrere Verantwortliche Art. 24

- Zukünftig mehrere Verantwortliche möglich, bisher nicht nach BDSG
- Forderung des Düsseldorfer Kreises 29.4.2010 wegen Cloud Computing
- Aufgabenverteilung mit Verantwortungsübernahme erforderlich
- Klärung der Rechte der Betroffenen in diesen Fällen, sonst gegenüber allen
- Kern der Vereinbarung muss Betroffenen mitgeteilt werden
- Bei unklarer Vereinbarung gesamtschuldnerische Haftung aller Verantwortlichen

Dokumentation

- Dokumentationspflicht in den Unternehmen (Artikel 28), schriftlich oder in nicht-lesbarer Form, die lesbar gemacht werden kann (z.B. elektronisch), Vorlagepflicht bei Aufsichtsbehörden
- Datenschutzkonzept nach Artikel 22
- Dokumentation Auftragsverarbeitung Artikel 26
- Sicherheitskonzept nach Artikel 30
- Ggf. Pflicht des Auftraggebers zur Erstellung einer Datenschutz-Folgenabschätzung nach Artikel 33 statt Vorabkontrolle
- Einrichtung verpflichtender Datenschutzbeauftragter (neue Grenzen)

Dokumentation Art. 28

- Dokumentationspflicht gilt für Verantwortliche und Auftragsdatenverarbeiter (neu)
- Verfahrensverzeichnis mit folgenden Angaben:
  - Name der verantwortlichen Stelle(n) inkl DSB
  - Zweck der Datenverarbeitung, berechtigtes Interesse nach 6 I f
  - Kategorien von Betroffenen und jeweils zugeordnet Datenkategorien
  - Empfänger von Daten, insbesondere im Ausland
  - Datenkategorien bei Datenübermittlung ins Ausland oder internationale Einrichtungen
  - Löschfristen
  - Technische und organisatorische Sicherheitsmaßnahmen, wenn möglich

Meldung von Sicherheitsvorfällen

- Unverzügliche Meldung an Aufsichtsbehörde Art. 31
- Detaillierte Vorgaben über den Inhalt der Meldung
- Meldung an die Betroffenen Art. 32
- **Bei Sicherheitskonzept und regelmäßiger Verschlüsselung der Daten nicht erforderlich**
- Verzeichnis bei Aufsichtsbehörde

Meldung von Vorfällen nach TKG

- § 109a TKG:
- **In Fällen, in denen in dem Sicherheitskonzept nachgewiesen wurde, dass die von der Verletzung betroffenen personenbezogenen Daten durch geeignete technische Vorkehrungen gesichert, insbesondere unter Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens gespeichert wurden, ist eine Benachrichtigung nicht erforderlich**.

Risiken Art. 33 I

- Verwendung neuer Technologien
- Hohes Risiko
  - Diskriminierung
  - Identitätsklau
  - Identitätsbetrug
  - Finanzielle Verluste
  - Imageschäden
  - Bruch von Pseudonymen
  - Verlust der Vertraulichkeit
  - Finanzielle oder soziale Nachteile
- Liste der Aufsichtsbehörde, wann und wann nicht Folgenabschätzung

Inhalte der Folgeabschätzung Art. 33

- allgemeine Beschreibung der geplanten Verarbeitungsvorgänge
- Berücksichtigung gesamter Lebenszyklus der Daten
- Bewertung der bestehenden Risiken in Bezug auf die Rechte und Freiheiten der betroffenen Personen
- Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen
- Verfahren zum Schutz personenbezogener Daten und zum Nachweis der Einhaltung der Vorgaben

Datenschutzaudit Art. 33a

- Bei Notwendigkeit einer Folgeabschätzung werden Audits erforderlich
- Prüfung des Datenschutzes spätestens 2 Jahre nach Folgeabschätzung
- Wiederholung des Audits alle 2 Jahre
- Datenschutzbeauftragter ist zu beteiligen
- Bisher § 9a BDSG, geplantes Gesetz dazu ist nie erlassen worden

Art. 39a Zertifizierungsstellen

- Neu im Entwurf Dezember 2014
- Prüfung durch Aufsichtsbehörden bzw Nationale Akkreditierungsstellen
- Akkreditierung setzt voraus:
  - Dokumentiertes Verfahren
  - Unabhängigkeit
  - Fachkunde
  - Beschwerdemanagement

- Akkreditierung kann entzogen werden
- Aufsichtsbehörden können Kriterien festlegen, EU-Kommission kann Rechtsakte erlassen

Haftung / Schadensersatz Art. 77

- Haftung sowohl des Verantwortlichen aus auch des Auftragsverarbeiters nach außen
- bisher nach BDSG nur Haftung des Verantwortlichen
- bei mehreren Verantwortlichen gesamtschuldnerische Haftung, es sei den Vereinbarung zur Aufgabenverteilung
- Exkulpation des Verantwortlichen oder des Auftragsverarbeiters , wenn er nachweist, dass ihn kein Verschulden trifft
- bisher Vermutung für Haftung des Verantwortlichen nach § 7 BDSG und Exkulpationsmöglichkeit

Sanktionshöhe

- Strafrechtlich nach Festlegung des Mitgliedsstaates
- Dez 2014: Verwaltungsstrafen bis 100 Millionen Euro oder 5 % des weltweiten Umsatzes, davon der höhere Betrag
- Juni 2015: max. 250.000 Euro oder 0,5% Jahresumsatz, davon der höhere Betrag
- Inhaber des europäischen Datenschutzsiegels werden nur bei nachgewiesenem Verschulden bestraft
- bisher Bußgelder in Deutschland bis 300.000 Euro bei materiellen Datenschutzverstößen und 50.000 Euro bei formellen Datenschutzverstößen

Vergleich mit IT-Sicherheitsgesetz

- Gesetz vom 17.7.2015, in Kraft seit 25.7.2015
- Erhöhung der IT-Sicherheit
- Meldepflichten von Sicherheitsvorfällen für Betreiber kritischer Infrastrukturen
- Sicherheitsaudits alle 2 Jahre für Betreiber kritischer Infrastrukturen
- Aufsichtspflichten des BSI
- Höhere Verfügbarkeitsanforderungen für Tele- und Mediendiensteanbieter

Kritische Infrastrukturen

Infrastrukturen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden

Sektoren Kritischer Infrastrukturen

Energie

Informationstechnik
und Telekommunikation

Wasser

Gesundheit

Transport
und Verkehr

Ernährung

Finanz- und Versicherungswesen

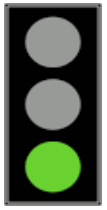
Neue Aufgaben des BSI

- Zentrale Stelle für die Sicherheit in der Informationstechnik kritischer Infrastrukturen
- Zentrale Stelle für die Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit zuständigen Stellen im Ausland
- Untersuchung von Sicherheitsprodukten
- Beratung von Betreibern kritischer Infrastrukturen

Bundesamt
für Sicherheit in der
Informationstechnik

Pflichten kritischer Infrastrukturen

Angemessene Vorkehrungen zum Schutz von




Verfügbarkeit Integrität Authentizität Vertraulichkeit

Spätestens 2 Jahre nach Inkrafttreten der Verordnung

Branchenstandards können von Betreibern und Verbänden vorgeschlagen werden und von BSI genehmigt in Zusammenarbeit mit Bundesamt für Katastrophenschutz und jeweiliger Aufsichtsbehörde

Sicherheitsaudits alle 2 Jahre verpflichtend

Erweiterte Pflichten nach § 109 TKG

- Zweijähriger Turnus der Prüfung des Sicherheitskonzeptes
- Beteiligung von Bundesnetzagentur und BSI
- Meldepflichten bei Störungen
- Bußgeld bei Nichteinhaltung § 149 TKG
- Information von BSI und ggf. Europ. Institutionen

Änderungen im ITSG für alle

- Erweiterte Missbrauchskontrolle nach § 100 TKG bei Datenschutz- und Datensicherheitsverletzungen
- Erweiterte Verpflichtung zu IT-Sicherheit beim Angebot von Tele- und Mediendiensten nach § 13 Abs. 7 TMG
- Empfehlung der Verwendung starker Verschlüsselung