Impulsvortrag "EU-Datenschutzgrundverordnung"

Pro! Hochschule Ulm, Erstes Treffen des Fachkreises-IT, 20. November 2012

Prof. Dr. Markus Schäffter, Hochschule Ulm

Allgemeiner Datenschutz: Das Recht auf informationelle Selbstbestimmung

Personenbezogene Daten genießen in der Europäischen Union einen besonderen gesetzlichen Schutz.

> Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen.
>
> EU-Richtlinie 95/46/EG

In Deutschland hat das Bundesverfassungsgericht 1983 im so genannten „Volkszählungsurteil“ aus den grundrechtlich geschützten Persönlichkeitsrechten (Recht auf allgemeine Handlungsfreiheit und Unantastbarkeit der Menschenwürde) das Prinzip des informationellen Selbstbestimmungsrechts abgeleitet:

> Nur wer mit hinreichender Sicherheit überschauen kann, welche ihn betreffende In-formationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner einigermaßen abzuschätzen vermag, kann aus eigener Selbstbestimmung planen und entscheiden.
>
> Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Aus-übung seiner entsprechenden Grundrechte verzichten.
>
> Auszug aus dem "Volkszählungsurteil" BVerfGE 65,1 von 1983

Status Quo: EU-Datenschutzrichtlinie und nationales Datenschutzrecht

Die aktuelle „Datenschutzrichtlinie“ 95/46/EG legt Mindeststandards für den Schutz personenbezogener Daten in Europa fest. Umgesetzt werden diese durch die nationalen Parlamente in Form nationaler Datenschutzgesetze.

Die Mindeststandards umfassen:

- Informations- und Auskunftsrecht
- Widerspruchsrecht des Betroffenen, insbesondere gegen Werbung
- Vertraulichkeit und Sicherheit
- Meldepflicht und Kontrollen
- Einschränkung der Übermittlung in Drittländer

Das Deutsche Bundesdatenschutzgesetz geht an vielen Stellen über die Mindeststandards hinaus:

- Umfassende Meldepflicht bzw. umfassende Dokumentationspflicht
- Ernennung eines betrieblichen Datenschutzbeauftragten schon bei Kleinstunternehmen
- Eingeschränkte Nutzung zu Werbezwecken
- Einwilligungen müssen schriftlich und freiwillig erfolgen (EU: „ohne Zwang“)

Entwurf einer europaweiten Datenschutz-Grundverordnung

Offizieller Titel: „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)".

Offizieller Diskussionsstand zum 25. Januar 2012:

- Recht auf Vergessenwerden und auf Löschung (Artikel 17)
  Das „Recht auf Vergessenwerden" wird auch als „digitaler Radiergummi" bezeichnet und beinhaltet das Recht auf eine spätere Löschung persönlicher Daten.
- Detaillierte Dokumentation (Artikel 28)
  Die Dokumentation erfordert Informationen, welche dem aktuellen Verfahrensverzeichnis gemäß BDSG weitgehend entsprechen.
- Sicherheit der Datenverarbeitung (Artikel 30)
  Risikoorientierte Auswahl geeigneter Schutzmaßnahmen
- Meldepflicht bei Datenschutzverstößen (Artikel 31 und 32)
  Umgehende und umfassende Information, erst der Aufsichtsbehörde und dann aller mutmaßlich Betroffenen.
- Datenschutz-Folgeabschätzung (Artikel 33)
  Erweiterung der Vorabkontrolle gemäß BDSG um eine Abschätzung der Risiken für den Betroffenen.
- Drakonische Bußgelder (Artikel 79)
  Bußgelder zwischen 100T EUR und 1 Mio. EUR , bereits bei mangelhafter Dokumentation / Datenschutzorganisation, d.h. bei fehlender Datenschutzstrategie, fehlender Datenschutz-Folgeabschätzung, oder inaktivem Datenschutzbeauftragten.

Recht auf Vergessenwerden (Artikel 17)

Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Löschung von sie betreffenden personenbezogenen Daten […] zu verlangen, speziell wenn es sich um personenbezogene Daten handelt, die die betroffene Person im Kindesalter öffentlich gemacht hat, sofern einer der folgenden Gründe zutrifft: […]

Mögliche Gründe sind:

- Die Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a stützte, oder die Speicherfrist, für die die Einwilligung gegeben wurde, ist abgelaufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung der Daten.
- Die betroffene Person legt gemäß Artikel 19 Widerspruch gegen die Verarbeitung ein.
- Die Verarbeitung der Daten ist aus anderen Gründen nicht mit der Verordnung vereinbar.

Fazit: Der Ansatz eines Rechts auf Löschung ist wegweisend für den Umgang mit persönlichen Daten im digitalen Zeitalter und wird kontrovers diskutiert. Es widerspricht der Alltagserfahrung („Das Internet vergisst nicht!").

Umfang der Dokumentation (Artikel 28)

Alle für die Verarbeitung Verantwortlichen, alle Auftragsverarbeiter sowie etwaige Vertreter von für die Verarbeitung Verantwortlichen dokumentieren die ihrer Zuständigkeit unterliegenden Verarbeitungsvorgänge.

Die Dokumentation enthält mindestens folgende Informationen:

- Name und Kontaktdaten des [Verantwortlichen] […]
- Name und Kontaktdaten eines etwaigen Datenschutzbeauftragten;
- Angaben über die Zwecke der Verarbeitung sowie […] über die von dem für die Verarbeitung Verantwortlichen verfolgten legitimen Interessen;
- eine Beschreibung der Kategorien von betroffenen Personen und der Kategorien der sich auf diese beziehenden personenbezogenen Daten;
- die Empfänger […] denen personenbezogene Daten aus dem von diesen verfolgtem legitimen Interesse mitgeteilt werden;
- gegebenenfalls Angaben über etwaige Datenübermittlungen in Drittländer […];
- eine allgemeine Angabe der Fristen für die Löschung der verschiedenen Datenkategorien;
- eine Beschreibung der [eingesetzten Testverfahren zur Überprüfung der Wirksamkeit der eingesetzten Verfahren] […]

Fazit: In Deutschland ist diese Form der Dokumentation bereits heute zwingend erforderlich, vgl. §4 e i.V.m. § 4f BDSG. Die Verfahrensverzeichnisse können übernommen werden, müssen jedoch substantiell ergänzt werden (siehe unten).

Sicherheit der Verarbeitung (Artikel 30)

Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter Berücksichtigung des Stands der Technik und der Implementierungskosten technische und organisatorische Maßnahmen, die geeignet sind, ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.

Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen im Anschluss an eine Risikobewertung die in Absatz 1 genannten Maßnahmen zum Schutz personenbezogener Daten vor unbeabsichtigter oder widerrechtlichen Zerstörung oder vor unbeabsichtigtem Verlust sowie zur Vermeidung jedweder unrechtmäßigen Verarbeitung, insbesondere jeder unbefugten Offenlegung, Verbreitung beziehungsweise Einsichtnahme oder Veränderung.

Fazit: Die Umsetzung angemessener technisch-organisatorischer Schutzmaßnahmen ist in Deutschland bereits heute zwingend erforderlich, vgl. § 9 BDSG (und Anlage). Dazu gehört seit der letzten Novellierung im Jahr 2009 zwingend der Einsatz kryptographischer Verschlüsselungs-verfahren bei der Datenübertragung über offene Netzwerke.

Meldepflicht bei Datenschutzverstößen (Artikel 31 und 32)

Bei einer Verletzung des Schutzes personenbezogener Daten benachrichtigt der für die Verarbeitung Verantwortliche die Aufsichtsbehörde ohne unangemessene Verzögerung und nach Möglichkeit binnen 24 Stunden nach Feststellung der Verletzung. Falls die Meldung an die Aufsichtsbehörde nicht binnen 24 Stunden erfolgt, ist dieser eine Begründung beizufügen.

Die Verantwortliche Stelle informiert zunächst umgehend die Aufsichtsbehörde umfassend über eingetretene Datenschutzverstöße, d.h. über den Umfang des Verstoßes, die Betroffenen und die Auswirkungen auf diese und die getroffenen reaktiven Maßnahmen.

Im Nachgang sind die Betroffenen zu informieren.

Der für die Verarbeitung Verantwortliche benachrichtigt im Anschluss an die Meldung nach Artikel 31 die betroffene Person ohne unangemessene Verzögerung von der Verletzung des Schutzes personenbezogener Daten, wenn die Wahrscheinlichkeit besteht, dass der Schutz der personenbezogenen Daten oder der Privatsphäre der betroffenen Person durch eine festgestellte Verletzung des Schutzes personenbezogener Daten beeinträchtigt wird.

Fazit: Diese Regelung geht deutlich über die bestehende Meldepflicht in § 42a BDSG hinaus, da die Meldepflicht nicht auf besonders sensitive Daten eingeschränkt ist.

Datenschutz-Folgeabschätzung (Artikel 33)

Bei Verarbeitungsvorgängen, die aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen, führt der für die Verarbeitung Verantwortliche oder der in seinem Auftrag handelnde Auftragsverarbeiter vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

Artikel 33 Absatz 2 nennt konkrete Beispiele, wann eine Datenschutz-Folgeabschätzung zwingend erforderlich ist:

- Bei der Bildung von Personenprofilen, beispielsweise zwecks Analyse ihrer wirtschaftlichen Lage, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens oder zwecks diesbezüglicher Voraussagen;
- Bei der Verarbeitung besonderer Daten im Sinne des BDSG: Gesundheit, ethnische Herkunft usw.
- Weiträumige Überwachung, insbesondere Videoüberwachung
- […]

Fazit: Der Ansatz einer Risikobewertung ist aus der Informationssicherheit wohl bekannt. Der Schritt hin zu einer risikoorientierten Betrachtung ist grundsätzlich richtig und begrüßenswert. Orientierung bietet der Standard ISO 27005 als Teil der ISO 27000-Familie (Informationssicherheitsmanagementsystem, ISMS). Ein gemeinsames Konzept zur Informationssicherheit und zum Datenschutz ist unbedingt anzustreben!

Bußgelder (Artikel 79)

Jede Aufsichtsbehörde ist befugt, nach Maßgabe dieses Artikels verwaltungsrechtliche Sanktionen zu verhängen.

Die verwaltungsrechtlichen Sanktionen müssen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Die Höhe der Geldbuße bemisst sich nach der Art, Schwere und Dauer des Verstoßes, seinem vorsätzlichen oder fahrlässigen Charakter, dem Grad der Verantwortung der natürlichen oder juristischen Person und früheren Verstößen dieser Person, den nach Artikel 23 eingeführten technischen und organisatorischen Maßnahmen und Verfahren und dem Grad der Zusammenarbeit mit der Aufsichtsbehörde zur Abstellung des Verstoßes.

Im Einzelnen sind folgende Höchstgrenzen für Bußgelder aufgeführt:

- Geldbuße bis zu 500 000 EUR bzw. bis in Höhe von 1 % des weltweiten Jahresumsatzes:
  - unvollständige / unverständliche Auskunft
  - Löschfristen nicht einhält
  - Auftragnehmer nicht ausreichend kontrolliert
  - nicht über eine vollständige Dokumentation verfügt
- Geldbuße bis zu 1 Mio EUR bzw. bis in Höhe von 2 % des weltweiten Jahresumsatzes:
  - keinen Vertreter benennt
  - keinen Datenschutzbeauftragten ernennt (ab 251 Mitarbeiter)
  - die Aufsichtsbehörde über Verstöße nicht informiert
  - keine Datenschutz-Folgenabschätzung vornimmt
  - Datenschutzsiegel missbraucht

Fazit: Die geplanten Höchstgrenzen für Bußgelder sind, verglichen mit dem Status Quo, drakonisch zu nennen und sollen die Unternehmen motivieren, den Datenschutz (noch) ernster als bisher zu nehmen!

Ein Datenschutzbeauftragter, zumindest in Teilzeit

Wer bereits über einen Datenschutzbeauftragten verfügt, sollte diesen sofort mit der Erweiterung der Dokumentation beauftragen. Bei der Durchführung von Risikoanalysen hilft ISO 27005.

Laut BDSG müssen nur Unternehmen einen Datenschutzbeauftragten ernennen, die mindestens 10 Mitarbeitende mit der Nutzung personenbezogener Daten betrauen. Die geplante EU-Verordnung verlangt dies von Unternehmen ab 250 Beschäftigten (egal mit welcher Tätigkeit betraut).

Jedoch machen auch dann die umfangreichen Dokumentationspflichten einen spezialisierten Datenschutzbeauftragten sinnvoll, auf jeden Fall in Teilzeit. Möglich ist, einen Mitarbeiter entsprechend fortzubilden oder einen externen Datenschutzbeauftragten zu ernennen.

Der Datenschutzbeauftrage *wirkt auf die Einhaltung der gesetzlichen Vorschriften hin* und *unterrichtet die Mitarbeiter* in Fragen des Datenschutzes. Er ist nicht für die Umsetzung zuständig, sondern unterstützt die Fachabteilungen mit Rat und Tat! (Quelle: BDSG)

Achtung: Wegen der Kontrollfunktion darf der Datenschutzbeauftragte nicht zur Leitungsebene gehören: Geschäftsführer, Personalleiter, IT-Leiter usw. sind tabu!

Aufgaben des Datenschutzbeauftragten gemäß EU-Datenschutzgrundverordnung: *Unterrichtung* der Mitarbeitenden, *Kontrolle* der Schutzmaßnahmen, *Ansprechpartner* für die Aufsichtsbehörde.

Hinweis: Dies entspricht im Wesentlichen den Aufgaben der Datenschutzbeauftragten nach dem BDSG mit erweiterten Kompetenzen bei Interventionen seitens der Aufsichtsbehörden.

Hinweis in eigener Sache: Die Hochschule Ulm bietet über die Technische Akademie Ulm eine Ausbildung zum/zur fachlich geprüften Datenschutzbeauftragten an: preisgünstig und effektiv: http://www.ta-ulm.de.

Referenzen

[95/46/EG] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:NOT

[EU-DSGV] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF

[TAU] Datenschutzausbildung der Technischen Akademie Ulm, www.ta-ulm.de

Zur Person des Vortragenden

Professor für Datenschutz und IT-Sicherheit an der Fakultät Informatik der Hochschule Ulm. Werdegang: promovierter Mathematiker, Spezialist für Internet-Sicherheit in der Telekommunikation, später für neue Sicherheitstechnologien im Finanzwesen, tätig als Unternehmensberater und als externer und interner Datenschutzbeauftragter.

Kontakt: schaeffter@hs-ulm.de; Tel. 0731/50-28012; www.hs-ulm.de/schaeffter