ARGE DATEN Privacy Austria

Tätigkeitsbericht 2015

ARGE DATEN
www.argedaten.at

Editorial

2015, das Jahr großer Datenschutz-Weichenstellungen. Zwei Ereignisse bleiben in Erinnerung: Zum einen das Safe-Harbor-Urteil des EuGH. Zum anderen, die nach jahrelanger Diskussion erzielte Einigung über den Wortlaut der neuen EU-Datenschutz-Grundverordnung. Auf nationaler Ebene sorgte das Staatsschutzgesetz für viel Diskussionsstoff, im Justizministerium dachte man laut über eine Neuauflage der Vorratsdatenspeicherung nach, ELGA startete in öffentlichen Krankenhäusern in Wien und in der Steiermark und Cybermobbing findet man seit Beginn des Jahres im Strafgesetzbuch.

„We have a deal!", ließ Jan Philipp Albrecht, Verhandlungsführer des Europäischen Parlaments für die EU-Datenschutz-Grundverordnung Mitte Dezember via Facebook verlautbaren. Ausgerechnet das soziale Netzwerk, das mit Inkrafttreten der EU-Datenschutzreform 2018 seine bisherigen Praktiken grundlegend verändern muss, war Überbringer der von vielen unerwarteten Botschaft. Aber was ändert sich für Facebook?

Europäische Facebook-Nutzer mussten sich bei Verstößen bislang an die irische Datenschutzbehörde wenden. Dass diese nicht gerade bemüht ist, Datenschutzverletzungen vor allem großer Unternehmen nachzugehen, zeigte nicht zuletzt der Fall Schrems. Unterschiedliche Datenschutzniveaus innerhalb der EU verhinderten bis dato eine effektive Rechtsdurchsetzung. Die EU-Datenschutz-Grundverordnung steht für Veränderung: In Zukunft können Betroffene jedenfalls bei der Datenschutzbehörde ihres Mitgliedstaates Beschwerden einbringen, unterschiedliche Datenschutzniveaus gehören dank einheitlicher Gesetzesauslegung der Vergangenheit an.

Dass große Unternehmen Datenschutzverletzungen in Zukunft nicht einfach einkalkulieren, ist ein weiteres Anliegen der EU-Datenschutz-Grundverordnung. Unternehmen drohen je nach Verstoß Bußgelder bis zu vier Prozent des weltweiten Jahresumsatzes oder 20 Millionen Euro. Das sind, zieht man den Jahresumsatz von Facebook oder Google heran, beträchtliche Summen. Wie ein von der Bürgerrechtsdachorganisation EDRi veröffentlichtes internes Dokument der irischen Ratspräsidentschaft zeigt, waren die irischen Vertreter nicht gerade begeistert von der Höhe der Strafen. Laut dem Bericht, ist zu überdenken, ob Verweise und Verwarnungen nicht sinnvoller seien. Nur ein Beispiel, wie die Granden der IT-Industrie bei den jahrelangen Verhandlungen ihre Finger im Spiel hatten.

Nicht nur standortpolitisch muss sich Facebook und Co mit Inkrafttreten der EU-Datenschutz-Grundverordnung etwas einfallen lassen. Ein wesentliches Ziel der Regelung ist die Stärkung der Nutzerrechte. So wurden die vom EuGH in seinem Google-Spanien-Urteil herausgearbeiteten Grundsätze für das Recht auf Vergessen in den Gesetzestext aufgenommen. Neben weitgehenden Informationspflichten wird das Recht auf Datenportabilität dem Nutzer mehr Kontrolle über seine Daten geben. Wollen Nutzer den Anbieter wechseln, müssen die personenbezogenen Daten kostenfrei und in einem allgemein nutzbaren Format übermittelt werden.

ARGE DATEN unterstützt Mitglieder

Abgerundet wird die Stärkung der Nutzerrechte durch das in Art. 76 DS-GVO normierte Verbandsklagerecht. Betroffenen wird ermöglicht, gemeinnützige Datenschutzorganisationen zu beauftragen, ihre Rechte durchzusetzen. Auch nach der Ablösung des DSG 2000 durch die EU-Datenschutz-Grundverordnung steht die ARGE DATEN mit Rat und Tat zur Seite um Mitglieder bei der Durchsetzung ihrer Rechte einerseits und der Einhaltung ihrer Pflichten andererseits bestmöglich zu unterstützen.

Apropos Pflichten. Für Unternehmen bedeutet die Erlassung der EU-Datenschutz-Grundverordnung einen Schritt weg von behördlichen Meldepflichten, hin zu mehr Eigenverantwortung. Jeder Auftraggeber hat eine Übersicht über die unternehmenseigenen Datenanwendungen zu führen und für gewisse Datenanwendungen ist das Risiko im Zuge von Datenschutz-Folgeabschätzungen zu bewerten. Unter Umständen besteht die Pflicht zur Bestellung eines Datenschutzbeauftragten.

Mit ARGE DATEN am Puls der Zeit

Über bestehende und zukünftige europarechtliche Herausforderungen informiert unser Seminar Datenschutz EU-Grundverordnung & Praxis am 21. April 2016. Schwerpunkt des Seminars sind Erfahrungen betrieblicher Datenschutzbeauftragter und Umsetzungsfragen des Datenschutzes aus internationaler Perspektive. Zentrales Thema ist neben geltendem Recht auch die neue EU-Datenschutz-Grundverordnung.

Ein steigender Mitgliederstand und unsere gut besuchten Seminare und Schulungen im Jahr 2015 zeugen von der Qualität unserer Arbeit. Wir sind überzeugt: Datenschutz soll kein zusätzliches bürokratisches Mühsal für Unternehmen darstellen und schon gar keine Innovations- oder Ideenbremse sein. Um am Ende des Tages eine rechtlich solide Lösung am Tisch liegen zu haben, muss der Datenschutz bereits am Morgen mitgedacht werden. Datenschutzbewusste Unternehmen sind gut beraten, sich schon jetzt auf die neue Rechtslage vorzubereiten.

Übrigens: Es gibt viele Möglichkeiten unser Anliegen und unsere Überzeugungen zu unterstützen. Durch eine Spende, durch Ihren Mitgliedsbeitrag oder durch Ihre praktische Mitwirkung bei unseren Veranstaltungen.

Philipp Hochstöger
ARGE DATEN - Privacy Austria

DATENSCHUTZ-STENOGRAMM 2015

EuGH erklärt Safe-Harbor-Abkommen für ungültig

Mikl-Leitner spricht sich für Vorratsdatenspeicherung nach deutschem Vorbild aus

Facebook verpasst sich umstrittene Nutzungsbedingungen

Staatsschutzgesetz wird von Regierung vorgestellt und sieht 10 Geheimdienste für Österreich vor

Smart-Meter Abmeldung auf Grund von Rechtsunsicherheit schwierig

OGH: Onlinemedien zur Aktualisierung personenbezogener Berichte verpflichtet

EU-Datenschutz-Grundverordnung wird nach Ende der Trilog-Verhandlungen vom Ausschuss für Bürgerrechte, Justiz und Inneres angenommen

Staatsschutzgesetz stellt mit unbestimmten Begriffen und weitreichenden Befugnissen eine Gefahr für Bürgerrechte dar

Samsung warnt Nutzer, Privates vor Smart-TV zu besprechen

ELGA startet in öffentlichen Spitälern in Wien und der Steiermark

Datenschutzrat spricht sich für Quick-Freeze statt Vorratsdatenspeicherung aus und warnt vor Einführung der Fluggastdatenspeicherung

OGH: Widerspruchsrecht nach § 28 Abs. 2 DSG 2000 wegen Verletzung des Rechts auf Meinungs- und Informationsfreiheit verfassungswidrig

ELGA-Start für niedergelassene Ärzte wird auf Mitte 2017 verschoben

Fluggastdaten: Innenausschuss des EU-Parlaments stimmt Richtlinie zur Sammlung europäischer Fluggastdaten zu

Klage von Max Schrems gegen Facebook in Wien zulässig

Inhalt

Ausbildungsreihe Betrieblicher Datenschutzbeauftragter

Die betrieblichen Datenschutzanforderungen werden zunehmend komplexer. Die neue EU-Grundverordnung Datenschutz überträgt den Betrieben mehr Verantwortung und mehr Dokumentationspflichten - Mit dieser Ausbildungsreihe bietet die ARGE DATEN eine umfassende Schulung http://seminar.e-monitoring.at/dsb

Warum „betrieblicher Datenschutzbeauftragter“?

Viele Unternehmen, insbesondere ab einer Größe von 50 Mitarbeitern, haben sich schon jetzt freiwillig entschlossen die Position eines „betrieblichen Datenschutzbeauftragten“ zu schaffen. Dies hat zahlreiche organisatorische Vorteile.

Mit der neuen EU-Grundverordnung Datenschutz sind ALLE öffentlichen Einrichtungen und viele Unternehmen verpflichtet einen „betrieblichen Datenschutzbeauftragten“ zu haben.

Durch die Schaffung dieser Position ergibt sich für alle Mitarbeiter eine klar dokumentierte Zuständigkeit für komplexe Datenschutzfragen. Damit wird die Koordination und Durchsetzung der notwendigen Datenschutzmaßnahmen erleichtert.

Der Datenschutzbeauftragte kann leichter Fristen und Verpflichtungen, die sich aus dem Datenschutzgesetz ergeben, wie die Registrierungspflichten (§ 17 DSG 2000), die Maßnahmen zur Datensicherheit (§ 14 DSG 2000), die Mitarbeiterschulung (§ 15 DSG 2000) oder den zeitgerechten Abschluss von Dienstleistervereinbarungen (§ 10 DSG 2000) koordinieren und überwachen.

Für Mitarbeiter, Kunden und Lieferanten ergibt sich eine eindeutige Kompetenzstelle für alle Datenschutzprobleme, unabhängig davon welche Geschäftsbereiche diese betreffen. Gerade Datenschutzfragen enthalten potentiellen Konfliktstoff, der durch eine rasche und effiziente Klärung offener Fragen professionell beseitigt werden kann.

Wie ist die Ausbildungsreihe organisiert?

Die Ausbildungsreihe besteht aus fünf in sich abgeschlossenen Modulen, die laufend angeboten werden. Die ersten vier Module können in beliebiger Reihenfolge besucht werden, das Abschlussmodul setzt den Besuch der anderen vier Module voraus.

Modul I:
Datenschutzgesetz Grundlagen
Termin: 19. April 2016

Modul II:
Datenverwendung im Unternehmen
Termin: 20. April 2016

Modul III:
Datenschutz und IT-Sicherheit
Termin: 3. Mai 2016

Modul IV:
Datenschutz EU-Grundverordnung & Praxis
Termin: 21. April 2016

Modul V: **Workshop: Datenschutzfragen im Betrieb identifizieren und lösen**
Termin: 4. Mai 2016

Hinweis: Jedes Modul ist in sich abgeschlossen. Wir behalten uns Verschiebungen der Detailinhalte und Änderungen in der Gewichtung aus aktuellen Anlässen oder sonstigen wichtigen sachlichen Gründen ausdrücklich vor.

Tätigkeitsbericht 2015

ARGE DATEN - Zertifikat

Nach erfolgreicher Absolvierung des Abschlussmoduls wird dem „betrieblichen Datenschutzbeauftragten" ein Zertifikat ausgestellt.

An wen wendet sich die Reihe?

Für Personen, die innerbetrieblich für Datenschutzfragen zuständig sind, insbesondere Mitarbeiter der IT-Abteilungen, der Revisions- und Rechtsabteilungen und Mitglieder der Geschäftsführung bietet die ARGE DATEN als vertiefende Schulung die Ausbildungsreihe zum „betrieblichen Datenschutzbeauftragten" an.

Weiters bietet die Reihe Betriebsräten eine ausgezeichnete Grundlage die Mitarbeiterrechte im Bereich betrieblicher Datenverarbeitung besser wahrzunehmen.

Die Reihe ist auch für selbständige IT-Berater, Juristen und Unternehmensberater geeignet, die kompetente Datenschutzberatung als zusätzliche Dienstleistung anbieten wollen.

Beispiele aus der Beratungspraxis der ARGE DATEN

- Handelsunternehmen: Übermittlung der Mitarbeiterliste an Konzernmutter
- Schuldnerberatung: Serververlagerung ins Ausland
- Industrieunternehmen: Werbung per SMS
- Softwareentwickler: Übermittlung der Strafregisterauszüge im Zuge einer Ausschreibung
- Versandhandel: Kundenauskunft ohne Kundennummer
- Gesundheitswesen: Datenschutzrechtliche Einordnung „Video-Dolmetsch"
- Industrieunternehmen: Newsletter mit Tracking der individuellen Reaktionen der Empfänger
- Arztpraxis: Passwörter für Arbeitsstationen
- Fachhochschule: Zulässigkeit von eMail-Werbung
- Verein: Einsatz einer IT-Ressourcenplanung für Mitarbeiter
- Industrieunternehmen: Video überwachung am Arbeitsplatz
- Maschinenbauunternehmen: Umgang mit eMails ausgeschiedener Mitarbeiter
- Transportunternehmen: Auswertung Personalfragebögen in der EU
- Versicherungsunternehmen: Videoüberwachung des Kundenparkplatzes durch Nachbarn
- Krankenhaus: Verschwiegenheitspflicht bei infektiösen Patienten
- Industrieunternehmen: Registrierung eines Informationsverbundsystems (Lieferantenmanagement)

Öffentlichkeitsarbeit, Informationsdienst

- Web-Service: rund 45.000 Besucher/Monat
- Newsletter: rund 5.000 Abonnenten
- Medienanfragen/-berichte: rund 600
- Mitgliederbetreuung/ Rechtshilfe: 93 (Google: Recht auf Vergessen, ELGA: Opt-Out, DSB-Beschwerdeverfahren: Recht auf Auskunft, Recht auf Löschung, Videoüberwachung: Illegale Videoüberwachung, Unzulässige Datenverwendung: Verstoß gegen §§ 6 DSG 2000)

Anfragen und Auskünfte betrafen folgende Bereiche:

25% Eingriffe in das Privatleben

17% Betrieb / Beruf / Anstellung

17% Behörden und Verwaltung

16% Finanzdienstleister / Wirtschaftsauskunftsdienste / Privatversicherer

8% Bildung

17% sonstige Anfragen

Veranstaltungen, InHouse Schulungen

60 Personen absolvierten 2015 die ARGE DATEN Ausbildungsreihe zum betrieblichen Datenschutzbeauftragten. Mit rund 600 TeilnehmerInnen waren unsere Datenschutzveranstaltungen sehr gut besucht.

Datenschutzthemen 2015

EU-Datenschutz-Grundverordnung – die Würfel sind gefallen

Mehr als vier Jahre sind vergangen, seitdem die damalige EU-Kommissarin Viviane Reding der Öffentlichkeit einen Entwurf für die EU-Datenschutz-Grundverordnung präsentiert hat. Nun ist es soweit: Die Verhandlungsführer der EU-Kommission, des EU-Parlaments und des Ministerrates konnten sich im Dezember auf den finalen Wortlaut des Gesetzestextes einigen. Nach der Abstimmung im Parlament wird die Verordnung zwei Jahre später in Kraft treten. Dabei sah es lange Zeit so aus, als wäre eine Einigung in weiter Ferne, in vielen grundlegenden Fragen bestand Uneinigkeit.

EIN Datenschutzstandard für 500 Millionen Bürger?

Ziel ist und war eine einheitliche Regelung für alle 28 Mitgliedstaaten. Jedoch ist der finale Entwurf geprägt von einem Kompromiss der EU-Institutionen: Während die EU-Kommission im Trilog auf eine direkt anwendbare einheitliche Verordnung drängte, verfolgte der Rat eher eine Taktik der Verwässerung, indem Mitgliedsstaaten in wichtigen Fragen erst recht wieder die Entscheidungskompetenz überlassen werden sollte.

Verpflichtender Datenschutzbeauftragter?

So vermisst man in der EU-Datenschutz-Grundverordnung eine einheitliche und klare Regelung bei der Frage ob die Ernennung eines Datenschutzbeauftragten verpflichtend sein soll oder nicht.

Im Entwurf der Kommission war von der verpflichtenden Ernennung eines betrieblichen Datenschutzbeauftragten die Rede, wenn ein Unternehmen mehr als 250 Mitarbeiter beschäftigt. Hingegen wollte der Rat den Gesetzgebern der Mitgliedstaaten die Entscheidung überlassen, ob sie einen verpflichtenden betrieblichen Datenschutzbeauftragten vorsehen oder nicht.

Der finale Text der EU-Datenschutz-Grundverordnung sieht die verpflichtende Ernennung für öffentliche Einrichtungen sowie für Unternehmen vor, deren Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen. Außerdem gilt die Bestellungspflicht für Unternehmen, zu deren Kerngeschäft der Umgang mit sensiblen Daten in erheblichem Umfang gehört. Ist die Verarbeitung von personenbezogenen Daten bloß Nebentätigkeit eines Unternehmens, muss ein betrieblicher Datenschutzbeauftragter jedenfalls nicht ernannt werden. Mitgliedstaaten können allerdings mit nationalen Gesetzen weitergehende Fälle vorsehen.

Auch nach Inkrafttreten der EU-Datenschutz-Grundverordnung entscheiden weitgehend die mitgliedstaatlichen Gesetzgeber, ob ein betrieblicher Datenschutzbeauftragter bestellt werden muss oder nicht. Eine Vereinheitlichung kann damit nicht erreicht werden.

Übrigens: Die EU-Datenschutz-Grundverordnung überlässt es den Unternehmen als Datenschutzbeauftragten einen Externen oder einen Mitarbeiter zu bestellen. Allerdings dürfen seine sonstigen Tätigkeiten nicht in einem Interessenkonflikt zu seiner Tätigkeit als betrieblicher Datenschutzbeauftragter stehen. Gleichzeitig verlangt die EU-Datenschutz-Grundverordnung vom Datenschutzbeauftragten Expertenwissen, das er im Betrieb unabhängig zur Erfüllung seiner Pflichten und Aufgaben einsetzen soll. Ein EDV-Mitarbeiter wäre prädestiniert als Datenschutzbeauftragter. Fraglich ist allerdings, ob nicht in vielen Fällen ein Interessenkonflikt mit seiner Tätigkeit zu erwarten und eine Ernennung folglich unzulässig ist.

Bußgelder

Das Parlament hat sich mit seiner Forderung nach einer massiven Erhöhung der Bußgelder weitgehend durchgesetzt. Die EU-Datenschutz-Grundverordnung sieht Bußgelder bis zu vier Prozent des weltweiten Jahresumsatzes oder 20 Millionen Euro vor. Obwohl das Parlament ursprünglich bis zu fünf Prozent gefordert hatte, sind die Bußgelder verglichen mit derzeit geltendem Recht sehr hoch angesetzt. Ob in der Praxis tatsächlich höhere Strafen verhängt werden, wird vor allem davon abhängen, ob die EU-Datenschutz-Grundverordnung eine wirksame welt- und nicht nur

europaweite Rechtsdurchsetzung gewährleisten kann.

Gültige Zustimmung

Die Datenschutz Grundverordnung legt in Art. 6 fest, wann die Verarbeitung personenbezogener Daten rechtmäßig ist. So müssen beispielweise Internet-User der Weiterverarbeitung ihrer Daten zustimmen, wenn nicht eine der übrigen Bedingungen erfüllt ist (z.b. Verarbeitung ist für die Erfüllung einer gesetzlichen Verpflichtung notwendig). Fehlt eine Einwilligung und ist auch nicht eine der übrigen Bedingungen erfüllt, ist die Verarbeitung der Daten nicht rechtmäßig.

Die am Trilog beteiligten Institutionen, hatten unterschiedliche Auffassung davon, was unter einer Einwilligung zu verstehen ist, konnten sich jedoch schließlich einigen: Eine wirksame Zustimmung bedarf einer zustimmenden Handlung. Sie muss informiert und für den Einzelfall erteilt werden. Insbesondere sind stillschweigende Zustimmungen nicht ausreichend. Die Befürchtung, das Niveau der EU-Datenschutz-Grundverordnung bezüglich der Zustimmung würde unter derzeit geltendes Recht fallen, tritt somit nicht ein.

Prinzip der Zweckbindung

Nach § 6 Abs. 1 Z 2 DSG 2000 dürfen Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden (Prinzip der Zweckbindung). Der Grundsatz der Zweckbindung setzt einerseits Auftraggebern Grenzen bei der Ermittlung von Daten, da diese

Der Weg zur EU-Datenschutzreform

März oder April 2016
Das Parlament stimmt im Frühjahr 2016 über den vereinbarten Gesetzestext ab. Zwei Jahre nach ihrer Publikation im Amtsblatt der EU ist die Datenschutz-Grundverordnung anwendbar.

17. Dezember 2016
Der vereinbarte Kompromiss wird von den Mitgliedern des zuständigen Ausschusses für Bürgerrechte, Justiz und Inneres angenommen.

15. Dezember 2016
Rat und Europäisches Parlament gelangen nach den abschließenden Verhandlungen zu einer Einigung. Der Gesetzestext der EU-Datenschutz-Grundverordnung steht fest.

Juli-Dezember 2016
In zahlreichen Trilog-Sitzungen wird Kapitel für Kapitel der EU-Datenschutz-Grundverordnung besprochen um einen Kompromiss zu finden. Ein schwieriges Unterfangen, in zahlreichen grundlegenden Fragen stehen sich unterschiedliche Auffassungen gegenüber.

24. Juni 2015
Erste koordinierende Trilog-Sitzung zur EU-Datenschutz-Grundverordnung zwischen EU-Kommission, EU-Parlament und EU-Rat.

15. Juni 2015
Der Rat der Justiz- und Innenminister aller 28 EU-Staaten macht mit Beschluss der allgemeinen Ausrichtung zur EU-Datenschutz-Grundverordnung den Weg frei für die Trilog-Verhandlungen. Im Rahmen des Trilogs soll nun die endgültige Fassung der EU-Datenschutz-Grundverordnung ausgearbeitet werden.

12. März 2014
Das Europäische Parlament bestätigt mit großer Mehrheit das im LIBE-Ausschuss beschlossene Verhandlungsmandat zur neuen EU-Grundverordnung Datenschutz (621 JA-Stimmen, 10 NEIN-Stimmen und 22 Enthaltungen. Aus österreichischer Sicht interessant: Abgeordneter Mölzer hat zu Datenschutz anscheinend keine Meinung und findet sich in guter Gesellschaft mit Le Pen. Abgeordneter Stadler ist gegen einen verbesserten Datenschutz).

21. Oktober 2013
LIBE-Ausschuss erteilt dem Europäischen Parlament den Auftrag für Verhandlungen mit dem Rat der Europäischen Union.

April 2013
Insgesamt werden mehr als 3.000 Änderungsvorschläge von Europaparlamentariern an der DS-GVO eingebracht.

16. Jänner 2013
Der federführende Berichterstatter des Europaparlaments zur DS-GVO, Jan Philipp Albrecht, präsentiert seinen Entwurf für Änderungsvorschläge.

25. Jänner 2012
Die Europäische Kommission präsentiert einen Vorschlag für die Neuordnung des Europäischen Datenschutzrahmens. Eine EU-Datenschutz-Grundverordnung (DS-GVO) soll die bisherige Datenschutzrichtlinie ersetzen.

nur für vorher festgelegte Zwecke gesammelt werden dürfen. Andererseits bietet der Grundsatz auch gewisse Flexibilität, indem er die Weiterverwendung der Daten für Zwecke erlaubt, die mit den vorher festgelegten Zwecken vereinbar sind.

Durch den Vorschlag des EU-Rats wäre der Grundsatz der Zweckbindung zumindest abgeschwächt worden. Der finale Text hält am Prinzip der Zweckbindung fest, eine Verarbeitung der personenbezogenen Daten für andere Zwecke ist nur zulässig, wenn der andere Zweck mit dem ursprünglichen kompatibel ist. Gleichzeitig werden Kriterien aufgezählt, wann ein Zweck kompatibel ist. So kommt es zum Beispiel darauf an, ob sensible Daten verarbeitet werden oder nicht.

Einheitliche Rechtsdurchsetzung: Europäischer Datenschutzausschuss

Einig waren sich die am Trilog beteiligten Institutionen in der grundsätzlichen Ausgestaltung des sogenannten europäischen Datenschutzausschusses. Dieser soll aus den Leitern bzw. Vertretern der nationalen Aufsichtsbehörden und dem europäischen Datenschutzbeauftragten bestehen. Der europäische Datenschutzausschuss hat sicherzustellen, dass die Verordnung einheitlich angewandt wird.

Unklar war, welche Rechtsqualität die Beschlüsse des europäischen Datenschutzausschuss haben werden. Während aus der Position des Rats hervorging, dass die Beschlüsse bindend sein sollen, war dies aus den Vorschlägen der Kommission und des Parlaments nicht unmittelbar ersichtlich. Nun ist es fix: Der europäische Datenschutzausschuss kann ähnlich dem Wettbewerbsrecht auch rechtlich bindende Entscheidungen treffen können und somit außerhalb des Einflusses der EU-Kommission für die einheitliche Anwendung der EU-Datenschutz-Grundverordnung sorgen. Sind sich nationale Aufsichtsbehörden uneinig, ist der europäische Datenschutzausschuss am Zug.

Ein fester Ansprechpartner? Kommt der „One-Stop-Shop“?

Unter dem Regime der Datenschutzrichtlinie war die Rechtslage für Unternehmen, die in mehreren Staaten der EU Niederlassungen unterhalten und dort Daten verarbeiten, kompliziert. Zuständig war bis dato die Datenschutzbehörde des jeweiligen Mitgliedsstaates. Dieser Umstand wird sich künftig mit dem „one-stop-shop“-Mechanismus ändern. Unternehmen werden es künftig einfacher haben, da sie nur mehr mit der Datenschutzbehörde jenes Mitgliedstaats kooperieren müssen, in dem sich der Hauptsitz des Unternehmens befindet. Bürger können sich unabhängig davon, wo der Datenmissbrauch erfolgt ist, an die die Datenschutzbehörde in Ihrem Mitgliedstaat wenden.

Eine erste Einschätzung

Das Verhandlungsergebnis kann sich sehen lassen, auch wenn wirkliche Innovationen ausgeblieben sind. Aus einem ungemein intransparenten Trilog-Verfahren, das für Bürger durch ungewollte Leaks zumindest ein wenig transparenter wurde, kann etwas Brauchbares herauskommen. Zwar liegt es in der Natur der Sache, dass das Produkt des informellen Trilogs ein Kompromiss ist. Man muss den Protagonisten, die sich für eine Stärkung des europäischen Datenschutzes eingesetzt haben, jedoch zuerkennen, dass sie in wichtigen Punkten vor wirtschaftlich übermächtigen Gegenspielern nicht eingeknickt sind.

Dauerbrenner Vorratsdatenspeicherung

2014 erlebten Verfechter der anlasslosen Bürgerüberwachung mit der Aufhebung der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung einen herben Rückschlag. Der EuGH hat in seinem Urteil zur Aufhebung der Vorratsdatenspeicherung klargestellt, dass Überwachungsgesetze ein legitimes Ziel verfolgen, dass sie aber auch verhältnismäßig sein müssen. 2015 scheint die Niederlage vergessen zu sein. Sowohl auf europäischer als auch auf nationalstaatlicher Ebene wurde 2015 der Weg für neue Gesetze zur Vorratsdatenspeicherung geebnet.

Mangels europäischer Regelung nehmen Mitgliedstaaten das Zepter zunehmend selbst in die Hand.

In Deutschland wurde dieses Jahr ein neues Gesetz zur Vorratsdatenspeicherung beschlossen. Das Gesetz ist nicht so eingriffsintensiv wie das Vorgängergesetz, das 2010 vom deutschen Bundesverfassungsgericht, aufgehoben worden war. Verkehrsdaten werden zehn Wochen, Verbindungsdaten vier Wochen gespeichert. Das Vorgängergesetz sah eine deutlich längere Aufbewahrung vor. Dennoch kündigten Gegner bereits Verfassungsbeschwerden an.

In Frankreich wurde die Vorrats-

datenspeicherung zum Zweck der Terrorismusbekämpfung bereits 2006 eingeführt. Zwei schreckliche Anschläge in Paris innerhalb eines Jahres zeigen die mangelnde Effektivität einer anlasslosen Bürgerüberwachung und machen klar, dass die Vorratsdatenspeicherung kein geeignetes Mittel zur Terrorbekämpfung darstellt.

Nichts desto trotz wird auch in der österreichischen Bundesregierung über einen neuen Anlauf für ein Gesetz laut nachgedacht. Justizminister Brandstätter spricht sich für ein „vernünftiges Maß" an Vorratsdatenspeicherung aus. Auch Innenministerin Mikl-Leitner ist alles andere als abgeneigt und strebt eine Lösung nach deutschem Vorbild an.

Gut möglich, dass die Mitgliedstaaten durch einen Rechtsakt der EU zum Handeln verpflichtet werden. In einer Sitzung des Rates für Justiz und Inneres Anfang Dezember zeigt sich die Mehrzahl der Delegationen einer neuen europaweiten Regelung jedenfalls nicht abgeneigt, nach dem Motto: „Wenn schon Vorratsdatenspeicherung, dann eine europaweit einheitliche."

Eine Vorratsdatenspeicherung der Nationalstaaten kann den Zweck der Terrorismusbekämpfung sicherlich nur unzureichend erfüllen. Eine einheitliche Vorgabe der EU würde zumindest mehr Sinn machen, als 28 unterschiedliche Gesetze. Es wird jedoch verkannt, dass eine Vorratsdatenspeicherung niemals das gelindeste, zum Ziel führende Eingriffsmittel eines Staates in die Privatsphäre ihrer Bürger darstellen kann. Viel sinnvoller als die Speicherung personenbezogener Daten sämtlicher Bürger auf Vorrat, wäre das sogenannte Quick-Freeze-Verfahren, bei dem entsprechende Daten nur von verdächtigen Personen gespeichert und bei richterlicher Genehmigung an die Behörden übermittelt werden. Damit eine europarechtliche Regelung zur Vorratsdatenspeicherung nicht wieder vom EuGH aufgehoben wird, ist für den europäischen Gesetzgeber bei der Ausgestaltung einer Richtlinie jedenfalls besondere Vorsicht und Fingerspitzengefühl gefragt.

Fluggastdatenspeicherung – Placebo für mehr Sicherheitsgefühl?

Fingerspitzengefühl kann man dem europäischen Gesetzgeber bei der Ausgestaltung der viel diskutierten EU-Richtlinie zur Fluggastdatenspeicherung (PNR) nicht nachsagen. 2013 lehnte das europäische Parlament einen Vorschlag wegen Grundrechtsbedenken noch ab.

Im Dezember 2015 sah die Sache plötzlich anders aus. Nach den Anschlägen in Paris knickte das EU-Parlament vor den Regierungen ein, der zuständige Innen- und Justizausschuss segnete das Vorhaben ab. Stimmt das europäische Parlament zu, werden künftig Passagierdaten wie Name, Reiseroute, Gepäcks- und Ticketinformationen und Zahlungsdaten für zumindest 6 Monate gespeichert. Das gilt jedenfalls für Flüge aus und in Drittstaaten. Für innereuropäische Flüge wäre die Erlassung eines nationalen Gesetzes notwendig.

Beschäftigungspolitik für Grundrechtsgerichte?

Sowohl eine europäische als auch eine nationale Regelung, die die anlasslose Speicherung von Passagierdaten vorsieht, ist nicht geeignet einen sinnvollen Beitrag zur Terrorbekämpfung zu leisten. Darüber hinaus ist eine anlasslose Speicherung unverhältnismäßig und mit voraussichtlichen Kosten von 500 Millionen Euro extrem teuer. Es ist wohl nur eine Frage der Zeit bis die Richtlinie vor dem EuGH landet und auf ihre Grundrechtskonformität geprüft wird. Es wäre ja nicht das erste Mal, dass der EuGH eine massenhafte und anlasslose Speicherung personenbezogener Daten für grundrechtswidrig erklärt.

http://www.argedaten.at/php/cms_monitor.php?q=VORRATSDATENSPEICHERUNG


© Sabine Meyer/ PIXELIO

EuGH-Urteil C-362/14 Safe-Harbor ist Geschichte

Mit dem Urteil C-362/14 hat der Europäische Gerichtshof das Safe-Harbor-Abkommen zwischen der Europäischen Union und den USA für ungültig erklärt. Dem Urteil wurde große Beachtung geschenkt, stützten doch viele Unternehmen bis dato Ihre Datenübermittlungen auf die Selbstzertifizierung US-amerikanischer Unternehmen.

Zur Ausgangslage

Wie bei allen Facebook-Nutzern mit Wohnsitz in der EU, werden auch die Daten von Max Schrems, von der irischen Tochtergesellschaft von Facebook, ganz oder teilweise an Server in die USA übermittelt und dort verarbeitet. Gestützt auf die Enthüllungen von Edward Snowden, legte Max Schrems Beschwerde bei der irischen Datenschutzbehörde ein und argumentierte, dass das derzeitige Recht und die Praxis in den USA keinen ausreichenden Schutz vor der Überwachung durch amerikanische Behörden bieten würden. Die irische Datenschutzbehörde wies die Entscheidung mit der Begründung zurück, dass die in der Entscheidung 2000/520 der EU-Kommission enthaltene Safe-Harbor-Regelung den USA ein angemessenes Datenschutzniveau gewährleisten würde. Der irische High Court legte die Rechtssache schließlich dem EuGH mit der Frage vor, ob die Entscheidung 2000/520 der EU-Kommission eine nationale Datenschutzbehörde daran hindere im Einzelfall zu prüfen ob ein angemessenes Datenschutzniveau vorliegt und ob eine Datenschutzbehörde die Datenübermittlung gegebenenfalls aussetzen könne.

Die Eckpfeiler des EuGH-Urteils

1. Die Entscheidung 2000/520 der EU-Kommission aus dem Jahr 2000 ist ungültig.
2. Auch wenn es eine Entscheidung der Kommission bezüglich der Angemessenheit des Datenschutzniveaus in einem Land gibt, sind nationale Aufsichtsbehörden zu der Prüfung befugt, ob ein angemessenes Datenschutzniveau tatsächlich vorliegt. Allenfalls ist der Datentransfer zu untersagen.

Bisherige Rechtslage in Österreich

In den §§ 12 und 13 DSG 2000 wird geregelt, wann eine genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland vorliegt und wann die Übermittlung oder Überlassung genehmigungsfrei ist. Grundsätzlich ist die Übermittlung und Überlassung von Daten an Empfänger in Vertragsstaaten des Europäischen Wirtschaftsraumes, sowie an Empfänger in Drittstaaten mit angemessenem Datenschutz genehmigungsfrei. Welche Drittstaaten angemessenen Datenschutz gewährleisten, wird in der Datenschutzangemessenheits-Verordnung (DSAV) festgestellt. Die USA findet man in der Aufzählung der DSAV nicht. Jedoch verweist die DSAV auf das Safe-Harbor-Abkommen. Übermittlungen und Überlassungen an US-Unternehmen, die sich im Wege einer Selbstzertifizierung den Grundsätzen des Safe-Harbor-Abkommens unterwarfen, waren genehmigungsfrei.

Konsequenzen des EuGH-Urteils

Stützte sich der Datentransfer ausschließlich auf die Selbstzertifizierung eines US-amerikanischen Unternehmens nach Safe-Harbor, muss nach der Aufhebung durch den EuGH ein Antrag auf Einzelgenehmigung bei der Datenschutzbehörde gestellt werden, falls keine der alternativen Rechtsgrundlagen zutreffen oder herangezogen werden können.

§§ 12 und 13 DSG 2000 sehen zahlreiche Alternativen für eine zulässige Datenübermittlung in die USA vor. Eine Datenübermittlung in die USA ist unter anderem genehmigungsfrei,
- wenn zulässigerweise veröffentliche Daten übermittelt werden (§ 12 Abs. 3 Z 1 DSG 2000),
- wenn Daten, die für den Empfänger nur indirekt personenbezogen sind, übermittelt werden (§ 12 Abs. 3 Z 2 DSG 2000),
- wenn ein eindeutig im Interesse des Betroffenen abgeschlossener Vertrag nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann (§ 12 Abs. 3 Z 6 DSG 2000),
- wenn die Übermittlung in einer Standardverordnung oder Musterverordnung ausdrücklich angeführt ist (§ 12 Abs. 3 Z 8 DSG 2000),
- wenn der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung seiner Daten ins Ausland gegeben hat (§ 12 Abs. 3 Z 5 DSG 2000).

Stimmt der Betroffene dem Datentransfer zu, entfällt das Genehmigungsverfahren bei der Datenschutzbehörde. Allerdings stellt sich bei den meisten Datenübermittlungen, vor allem im betrieblichen Bereich, die Frage, ob die Einholung der Zustimmung ein

taugliches Mittel darstellt. Abgesehen davon, dass die Einholung der Zustimmung aller Mitarbeiter/Kunden einen enormen Verwaltungsaufwand bedeutet, können Zustimmungserklärungen jederzeit widerrufen werden. Darüber hinaus wird die Einholung einer Zustimmung zum Beispiel bei Mitarbeiterdatenverarbeitungen auf Grund mangelnder Freiwilligkeit oft kein taugliches Mittel darstellen.

In der Post-Safe-Harbor-Ära können sich Unternehmen auch auf Standardvertragsklauseln und Binding Corporate Rules stützen. Im Genehmigungsverfahren kann die Datenschutzbehörde zusätzliche Sicherheitsvorkehrungen fordern, auch wenn Standardvertragsklauseln verwendet werden. Jedenfalls hat sie zu prüfen ob ein angemessener Datenschutz im konkreten Einzelfall vorliegt.

Einfluss des Urteils auf die EU-Datenschutz-Grundverordnung

Das EuGH-Urteil hat unmittelbaren Einfluss auf die EU-Datenschutz-Grundverordnung. Anders als die Entwürfe der EU-Institutionen, enthält der Text der finalen Fassung Anforderungen, die der EuGH im Safe-Harbor-Urteil aufgestellt hat.

Nach dem finalen Text der EU-Datenschutz-Grundverordnung soll die Kommission Abkommen regelmäßig überprüfen müssen. Überdies hat die Kommission bei der Beurteilung ob ein angemessenes Datenschutzniveau vorliegt, unter anderem das Recht der öffentlichen Sicherheit und Verteidigung, behördliche Zugriffsrechte auf personenbezogene Daten und die tatsächliche Umsetzung dieser Rechtslage zu berücksichtigen.

Privacy Shield – ein löchriges Datenschutzschild?

Anfang Februar haben sich die Europäische Kommission und die Vereinigten Staaten auf einen neuen Rahmen für die transatlantische Übermittlung von personenbezogenen Daten geeinigt.

Zwar steht der Wortlaut des Abkommens noch nicht fest, eines kann aber schon gesagt werden: Es ist äußerst fraglich ob die Kommission mit „Privacy Shield" den Anforderungen gerecht werden kann, die der EuGH in seinem Urteil aufgestellt hat und die auch in den Text der EU-Datenschutz-Grundverordnung aufgenommen wurden.

Solange die amerikanische Regierung nicht bereit ist, die bis dato sehr weitgehenden Gesetze zur Massenüberwachung zumindest einzuschränken, bleibt der grundrechtskonforme Abschluss eines „Safe-Harbor 2.0" nicht mehr als ein Wunschtraum der Verhandlungspartner. Die bloße Zusage von US-Vertretern, dass Daten der EU-Bürger künftig nicht der Massenüberwachung durch die USA unterliegen, ist rechtlich wertlos.


© Rainer Sturm / PIXELIO

ELGA unvollständige Gesundheitsakte startet in Spitälern

Nach jahrelangen Vorbereitungen und Diskussionen war es im Dezember 2015 soweit: ELGA startet. Zwar nur in öffentlichen Spitälern in Wien und der Steiermark – aber immerhin: Eigentlich hätte ELGA bereits Anfang 2015 in allen Landesspitälern starten sollen, der Start wurde jedoch verschoben.

Genauso lange wie über ELGA diskutiert wird, klärt die ARGE DATEN über die staatliche Zwangsdatenverarbeitung auf. Dabei wurden wir auch 2016 nicht müde darüber zu informieren, dass über jeden einzelnen Bürger ohne Zustimmung sensible Gesundheitsdaten verarbeitet werden.

Als Ziel von ELGA wird eine bessere Gesundheitsversorgung angegeben. In diesem Zusammenhang ist auch interessant welche Daten nicht von ELGA erfasst werden:

- *KEINE Röntgenbilder*
- *KEINE Magnetresonanzbilder*
- *KEINE Computertomographie bilder (CT)*
- *KEINE Ultraschallbilder*
- *KEINE Basisgesundheitsdaten wie Blutgruppe, Allergien, Medi - kamentenunverträglichkeiten und Impfungen*
- *KEINE medizinischen Aufzeichnungen der Hausärzte*
- *KEINE Gesundheitsakte der Spitäler*
- *KEINE Anamneseberichte*
- *KEINE Ergebnisse aus tele medizinischer Betreuung*
- *KEINE Aufbereitung von medzinischen Grunddaten, wie Cholesterinwerte, Blut- und Harnwerte*

ELGA würde alle Befunde und Entlassungsbriefe speichern, sagen die Befürworter. Sie verschweigen, dass unter „Befund“ und „Entlassungsbrief“ im medizinischen Alltag bloß die zusammenfassende Meinung eines Arztes zu verstehen ist, nicht jedoch die medizinischen Originaldaten. Kein Patient kann auf die tatsächlichen Aufzeichnungen bei Spitälern und Ärzten zugreifen.

Schon allein auf Grund der Tatsache, dass wichtige medizinische Unterlagen und Informationen fehlen, muss zwangsläufig die Frage gestellt werden, ob ELGA einer verfassungsrechtlich gebotenen Eignungsprüfung standhält. Das derzeitige System wird einer modernen Gesundheitsversorgung auch mangels Betriebssicherheit jedenfalls nicht gerecht.

„Opt-Out“ verfassungswidrig?

Darüber hinaus stellt sich die Frage ob das vom österreichischen Gesetzgeber im ELGA-G gewählte „Opt-Out“ mit dem Verfassungsrecht vereinbar ist. Nach § 1 Abs. 2 DSG sind „Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) genannten Gründen notwendig sind.“

Selbst wenn man annimmt, dass die Einführung einer elektronischen Gesundheitsakte für das „wirtschaftliche Wohl des Landes“ oder für den „Schutz der Gesundheit“ iSd Art. 8 Abs. 2 EMRK notwendig ist, darf nicht vergessen werden, dass nach § 1 Abs. 2 DSG auch im Falle einer zulässigen Beschränkung, der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden darf. Die Ausgestaltung von ELGA in der „Opt-Out“-Variante stellt mit Sicherheit nicht das gelindeste Mittel dar, hätte sich der österreichische Gesetzgeber doch auch für das „Opt-In“ entscheiden können. Bürger hätten sich bewusst anmelden müssen, um an ELGA teilzunehmen.

Dass eine elektronische Patientenakte nicht unbedingt als „Opt-Out“-System ausgestaltet sein muss, sieht man, wenn man einen Blick in andere EU-Länder wirft. So verlangen Länder wie Belgien, Frankreich, Italien oder Spanien, die ausdrückliche Einwilligung der Patienten bevor eine elektronische Patientenakte angelegt wird.

ELGA - Ausblick 2016

Schritt für Schritt sollen bis Ende 2016 alle öffentlichen Spitäler mit ELGA arbeiten. Doch auch in Zukunft enthält ELGA keine vollständigen medizinischen Originaldaten. Jeder Betroffene ist daher gut beraten an diesem System nicht mitzumachen und sollte sich abmelden. Die ARGE DATEN hat dazu ein einfaches Formular entwickelt, mit dem die Abmeldung ohne großen Aufwand möglich ist.

Details zum ELGA-Opt-Out finden sich unter Was für den ELGA Widerspruch („OptOut“) tun?, das Formular kann unter http://ftp.freenet.at/privacy/muster/elga-optout.doc abgerufen werden.

mehr: unter http://www.argedaten.at/php/cms_monitor.php?q=E-CARD

Cybermobbing als neuer Straftatbestand

Cybermobbing stellt für Betroffene eine extreme Belastung dar. Werden Aufnahmen aus dem höchstpersönlichen Lebensbereich ins Internet gestellt, sind sie einer breiten Öffentlichkeit zugänglich. Ins Internet hochgeladene Fotos oder beleidigende Handlungen sind darüber hinaus meist über längere Zeit aufrufbar, sodass die bloßstellende Wirkung besonders lange andauern kann.

Das Phänomen „Cybermobbing“ war bis dato nur teilweise strafrechtlich erfasst, in Betracht kamen vor allem Ehrenbeleidigungsdelikte, Nötigung oder die pornographische Darstellung Minderjähriger. Durch das Strafrechtsänderungsgesetz 2015 soll sich das ändern: Cybermobbing als Straftatbestand wird unter dem Titel „Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems“ in das Strafgesetzbuch eingeführt und ist mit 1.1.2016 in Kraft getreten.

§107c StGB (1) Wer im Wege einer Telekommunikation oder unter Verwendung eines Computersystems in einer Weise, die geeignet ist, eine Person in ihrer Lebensführung unzumutbar zu beeinträchtigen, eine längere Zeit hindurch fortgesetzt
1. eine Person für eine größere Zahl von Menschen wahrnehmbar an der Ehre verletzt oder
2. Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereiches einer Person ohne deren Zustimmung eine für eine größere Zahl von Menschen wahrnehmbar

macht, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

(2) Hat die Tat den Selbstmord oder einen Selbstmordversuch der im Sinn des Abs. 1 verletzten Person zu Folge, so ist der Täter mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Zu den Tatbestandsmerkmalen

Wie aus den Erläuterungen zum Ministerialentwurf hervorgeht, ist der Begriff „im Wege einer Telekommunikation" sehr weit. Darunter versteht man den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten aller Art in Form von Zeichen, Sprache, Bildern oder Tönen. Insbesondere fallen E-Mails, SMS und Anrufe darunter. Ebenso ist die Tatbestandsverwirklichung des § 107c „unter Verwendung eines Computersystems" möglich.

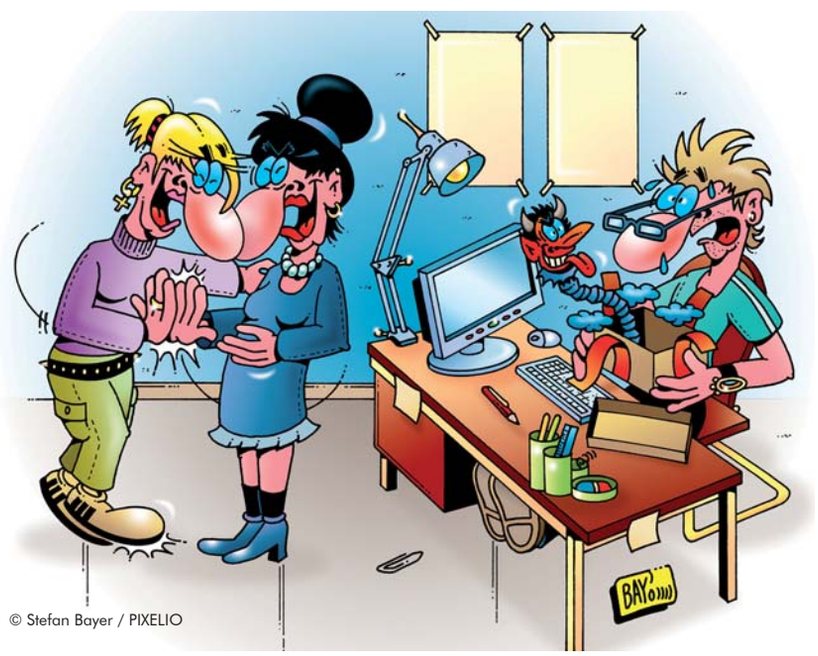
Die Tathandlungen müssen geeignet sein, die betroffene Person in Ihrer Lebensführung unzumutbar zu beeinflussen. Nach dem Willen des Gesetzgebers kommt es darauf an, ob das Verhalten derart unerträglich ist, dass auch ein Durchschnittsmensch in dieser Situation auf Grund der Handlungen möglicherweise seine Lebensgestaltung geändert hätte. Dass tatsächlich die Lebensführung beeinträchtigt wurde, ist nicht erforderlich. Bei der Bekanntgabe oder Veröffentlichung von Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereiches kann eine solche Eignung jedoch nur dann angenommen werden, wenn eine solche objektiv geeignet ist, das Opfer bloßzustellen.

Was unter dem Begriff „längere Zeit hindurch fortgesetzt" zu verstehen ist, hat sich, nach dem Willen des Gesetzgebers, an den Umständen des Einzelfalls zu orientieren. In manchen Fällen genügt es, wenn jemand eine Belästigung im Sinne § 107c StGB einmalig begeht. Werden beispielweise Nacktfotos einer Person ohne Zustimmung ins Internet hochgeladen und die Fotos über längere Zeit nicht gelöscht, wird eine Strafbarkeit bei Vorliegen der übrigen Voraussetzungen gegeben sein. Andererseits wird man bei Belästigungen durch E-Mails, SMS oder Telefonanrufe erst bei wiederholten Tathandlungen von „über längere Zeit fortgesetzt" sprechen können. Der Gesetzgeber sieht derartige Eingriffe als weniger massiv an. Das Opfer wird sich den Belästigungen durch SMS oder dergleichen leichter entziehen können.

Die drei genannten Tatbestandsmerkmale müssen kumulativ vorliegen. Zusätzlich muss die Person „für eine größere Zahl von Menschen wahrnehmbar an der Ehre verletzt" oder „Tatsachen oder Bildaufnahmen des höchstpersönlichen Lebensbereiches einer Person ohne deren Zustimmung für eine größere Zahl von Menschen wahrnehmbar" gemacht worden sein.

Unter Verletzung der Ehre versteht der Gesetzgeber jede Verminderung des Ansehens und der Achtung einer Person in ihrem sozialen Umfeld. Es kommt darauf an, ob die Verletzung der Ehre objektiv nachvollziehbar ist.

Nach dem Willen des Gesetzgebers deckt sich der Begriff des „höchstpersönlichen Lebensbereiches" mit dem des Privat- und Familienlebens in Art. 8 EMRK. Dazu zählen unter anderem das Sexualleben, der sensible Bereich des Familienlebens, Krankheiten, Behinderungen und religiöse Ansichten. Es muss zusätzlich geprüft werden, ob die Drohung geeignet ist beim Betroffenen begründete Besorgnis auszulösen. Laut den Erläuterungen umfassen Bildaufnahmen des höchstpersönlichen Lebensbereichs neben Aufnahmen des Opfers auch dessen Wohnräume.



Fazit

Wie oft der neu eingeführte § 107c StGB zur Anwendung kommt, wird sich zeigen und insbesondere davon abhängen, wann Gerichte Belästigungen als geeignet ansehen, eine Person in ihrer Lebensführung unzumutbar zu beeinträchtigen. Ist das bereits der Fall wenn ein Arbeitnehmer aus einer WhatsApp-Gruppe ausgeschlossen wird, in der sich alle Arbeitskollegen befinden? Wenn jemand aus dem Computerspiel-Team ausgeschlossen wird? Derartige Sachverhalte unter Strafe zu stellen war sicher nicht im Sinne des Gesetzgebers.

Der Zweck des § 107c StGB liegt nicht in der Regelung alltäglicher gesellschaftlicher Konflikte, vielmehr sollten massive Persönlichkeitsverletzungen mit schwerwiegenden Folgen für Betroffene unter Strafe gestellt werden. So könnte zum Beispiel das Hochladen eines Nacktfotos in die WhatsApp-Gruppe mit 15 Personen bei Vorliegen aller Voraussetzungen nach § 107c strafbar sein. Ein beleidigender Kommentar auf Facebook wird meist noch keine Strafbarkeit begründen, wiederholte Beschimpfungen könnten sehr wohl strafbar sein. Allgemeine Fallgruppen aufzuzählen ist aber weniger sinnvoll, eine Einschätzung hat in jedem Einzelfall zu erfolgen.

Videoüberwachung im Umkleideraum

Man könnte meinen, bei Unternehmen bestehe mittlerweile ein Basis-Wissen über die datenschutzrechtlichen Grundlagen im Bereich der Videoüberwachung. Wie ein, an die ARGE DATEN herangetragener Fall zeigt, hat es sich noch zu wenig herumgesprochen, dass es für Videoüberwachungen schon seit der DSG-Novelle 2010 klare Regelungen gibt (nachzulesen unter http://www.argedaten.at/php/cms_monitor.php?q=VIDEO)

Zur Anzeige gebracht

Anfang 2015 wurden wir auf Videokameras in den Umkleideräumen einer steirischen Therme aufmerksam gemacht. Nach einem Blick ins Datenverarbeitungsregister fiel uns auf, dass keine Meldung vorhanden war. Wie sich herausstellte wurden auch keine Aufkleber oder dergleichen angebracht.

Nachdem die ARGE DATEN eine Anzeige bei der zuständigen Bezirksverwaltungsbehörde eingebracht hatte, sahen die Zuständigen ihr Fehlverhalten ein und nahmen die Überwachungsanlage außer Betrieb.

Pflichten kennen – Strafen vermeiden

Die Paragraphen 50a bis 50e DSG 2000 regeln ab wann man von einer Videoüberwachung spricht (§ 50a DSG 2000), wann diese gemeldet werden muss (§ 50c DSG 2000), wie diese zu kennzeichnen ist (§ 50d DSG 2000), wie aufgezeichnete Videodaten beauskunftet werden müssen (§ 50e DSG 2000) und auf was sonst noch im Betrieb geachtet werden muss (§ 50b DSG 2000).

§ 50d DSG 2000 sieht vor, dass jede Videoüberwachung in einer Art und Weise gekennzeichnet werden muss, dass jeder potentiell Betroffene, der sich einem überwachten Objekt nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen. Darüber hinaus, muss aus der Kennzeichnung (beispielsweise Aufkleber an der Eingangstür eines Geschäfts) auch der Auftraggeber der Videoüberwachung hervorgehen, soweit dieser nach den Umständen des Falles nicht bereits bekannt ist.

Sofern Videodaten digital aufgezeichnet werden, müssen Videoüberwachungen beim Datenverarbeitungsregister gemeldet werden. Ausnahmen stellen Videoüberwachungen dar, die entweder gar nicht, oder nur analog aufzeichnen oder sich im Rahmen der Standardanwendung SA032 „Videoüberwachung“ befinden.

Betroffene sollten sich wehren

Aufgrund des starken Eingriffes in die Privatsphäre hat der Gesetzgeber ganz klare Bestimmungen festgelegt wann und in welchem Rahmen Videoüberwachungen zulässig sind. Betroffene sollten illegale Videoüberwachungen nicht einfach dulden, sondern von ihren Rechten Gebrauch machen und Anzeige erstatten. Strafandrohungen von bis zu 10.000 Euro könnten einige Betreiber dazu bringen ihren Pflichten entweder nachzukommen oder die Videoüberwachung zu unterlassen.

Die ARGE DATEN hat dazu einen Musterbrief erstellt der es Betroffenen leichter machen soll ihre Rechte zu wahren. Den Musterbrief und die wichtigsten Informationen zur Videoüberwachung findet man unter: http://www.argedaten.at/php/cms_monitor.php?q=VIDEO

Salzburger Talentecheck

Auf www.talentecheck-salzburg.at steht geschrieben: „Der Talente-Check Salzburg ist eine Kooperation der Wirtschaftskammer Salzburg mit dem Land Salzburg und dem Landesschulrat für Salzburg. Jeder Mensch hat berufliche Wünsche und Träume, Fähigkeiten, Stärken und Talente. Je genauer man sich damit auseinandersetzt, umso leichter fällt der berufliche Weg. Nicht immer ist jedoch klar, wozu man berufen ist." Der Talente-Check Salzburg soll jugendlichen Schülern eine Orientierungshilfe bieten.

Nachdem die Eltern die Einverständniserklärung unterschrieben haben, wird der Talente-Check durchgeführt. Schüler führen Tests durch, bei denen ihre Stärken und Schwächen herausgefiltert werden. Anschließend findet ein Analysegespräch mit Psychologen statt. Dass dabei Daten der Schüler ermittelt und verarbeitet werden müssen, versteht sich von selbst, allerdings sollte von den Verantwortlichen nicht auf das Datenschutzgesetz 2000 und auf die vom OGH herausgearbeiteten Anforderungen an eine gültige Zustimmung vergessen werden.

So wandte sich eine Lehrerin an uns, die Bedenken bezüglich der Einverständniserklärung hatte. Es stellte sich heraus, dass die Einverständniserklärung aus mehreren Gründen mangelhaft ist:

Unter anderem sind die Datenarten in der Einverständniserklärung zu unbestimmt angeführt. Neben Daten wie Name, Geburtsdatum und Adresse werden die Testantworten zum Zweck der Durchführung des Talente-Checks gespeichert. Jedoch werden der Einverständniserklärung die Testfragen nicht beigelegt, der Fragebogen steht auch auf der besagten Website nicht zum Download zur Verfügung. Somit wissen Eltern nicht, welche Daten über Ihr Kind tatsächlich gespeichert werden.

Besonders kritisch zu betrachten ist, dass laut der Einverständniserklärung die Noten in den Hauptfächern ermittelt und zum Zweck der Durchführung des Talente-Checks verarbeitet werden. Nach § 7 Abs. 3 DSG 2000 setzt die Zulässigkeit einer Datenverwendung voraus, dass die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und dass die Grundsätze des § 6 eingehalten werden. Nach § 6 Abs. 3 Z 3 dürfen Daten nur verwendet werden, soweit sie für den Zweck der Datenanwendung wesentlich sind und über diesen Zweck nicht hinausgehen. Zusammengefasst kann man sagen: Die Speicherung und Verarbeitung der Noten der Schüler muss für den Zweck des Talente-Check notwendig und erforderlich sein. Ansonsten ist die Datenverarbeitung nicht zulässig.

Die Verarbeitung der Noten der Schüler zum Zweck eines Talente-Checks widerspricht geradezu den Grundsätzen einer zulässigen Datenverarbeitung nach §§ 7 Abs. 3 und 6 Abs. 3 Z 3 DSG 2000. Insbesondere ist nicht ersichtlich, wieso die Verarbeitung der Noten für einen Talente-Check eines Schülers notwendig und erforderlich sein soll. Die Verarbeitung der Noten wäre allenfalls für Lehrer interessant, um prüfen zu können ob Fähigkeiten und Noten der Schüler übereinstimmen. Das ist aus der Einverständniserklärung jedoch nicht ersichtlich.

Die Sinnhaftigkeit eines Talente-Checks für Jugendliche steht außer Frage. Jedoch dürfen nur die erforderlichen Daten verwendet werden, um nicht gegen die Grundsätze des Datenschutzgesetzes 2000 zu verstoßen. Da aus der Einverständniserklärung auch nicht ersichtlich ist, welche Daten verarbeitet werden und nicht klar erkennbar ist, wer die Daten verarbeitet, raten wir derzeit von der Teilnahme am Talente-Check Salzburg ab.

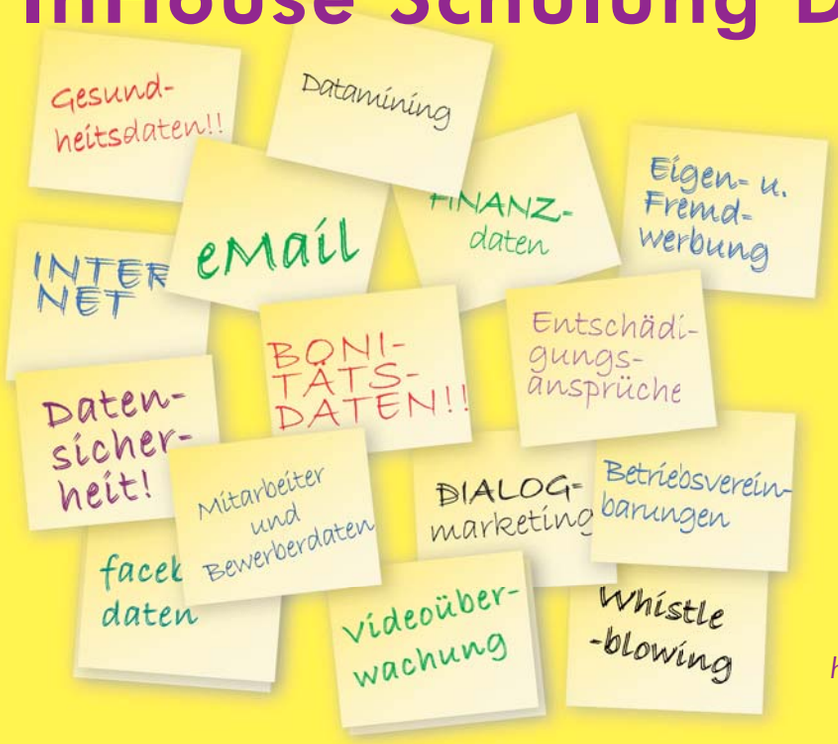
Impressum:

ARGE DATEN - Österr. Gesellschaft für Datenschutz
A-1160 Wien, Redtenbacherg. 20

Fon +43/676/9107032,
Fax +43/1/5320974
www.argedaten.at ,
info@argedaten.at
ZVR 774004629, DVR 0530794

Grundlegende Richtung:
Der Verein bezweckt die Erforschung von Wechselwirkungen zwischen EDV-Einsatz, Informationsrecht, Datenschutz und Gesellschaft (Auszug aus den Statuten §2 Abs.1).
Vorstand: Michael Krenn, Erwin Sulzgruber, Hans Zeger
Grafik: Charlotte Schönherr
Text: Philipp Hochstöger
Fotos: e-commerce monitoring GmbH, Sabine Meyer, Stefan Bayer, Rainer Sturm, pixelio.de

InHouse Schulung Datenschutz



Nutzen Sie die Vorteile einer InHouseschulung!

- ✓ *Datenschutz kommt zu Ihnen*
- ✓ *Modulares Konzept*
- ✓ *Unlimitierte Teilnehmerzahl*
- ✓ *Wir beantworten Ihre individuellen Datenschutzfragen*

Ihr individuelles Angebot:
info@e-monitoring.at
fon: +43 1 532 09 44
fax: +43 1 532 09 74
http://seminar.argedaten.at/inhouse

InHouse Schulung Datenschutz die Module

InHouse-Schulung A: DATENSCHUTZ BASIC
Behandelt werden die Grundbegriffe des Datenschutzes. Das Modul bietet allen Mitarbeitern einen ersten Einstieg in die Datenschutzmaterie. Ideal auch zur Datenschutz-Sensibilisierung für alle Mitarbeiter. (1,5 Stunden Vortrag) - Kosten 1.100,- (inkl. USt. 1.320,-) + Reiseaufwand*

InHouse-Schulung B: DATENSCHUTZ OVERVIEW
Neben den Grundbegriffen können weitere Datenschutzthemen vertiefend behandelt werden. Entscheiden Sie selbst und wählen Sie zwei Schwerpunkte aus der nebenstehenden Liste aus. Dauer: halbtags (3 Stunden Vortrag + 1 Kaffeepause) - Kosten 1.700,- (inkl. USt. 2.040,-) + Reiseaufwand*

InHouse-Schulung C: DATENSCHUTZ ENHANCED
Nach einer fundierten Einführung wird gezielt auf die spezifischen Probleme Ihrer Organisation eingegangen. Sei es im Umgang mit Kundendaten, Gesundheitsdaten, Bonitätsdaten oder Finanzdaten, im Personalwesen oder bei Data-Mining. Wählen Sie vier Schwerpunktthemen aus der untenstehenden Liste aus. Dauer: ganztags (6 Stunden Vortrag + Mittagspause und 2 Kaffeepausen) - Kosten 2.600,- (inkl. USt. 3.120,-) + Reiseaufwand *

Themenschwerpunkte

- ☐ Überblick allgemein
- ☐ Registrierung von Datenverarbeitungen
- ☐ Auskunfts- und Informationsrechte
- ☐ Internationaler Datenverkehr
- ☐ Videoüberwachung
- ☐ Betriebsvereinbarung Datenschutz
- ☐ Internet/eMail und Datenschutz
- ☐ Datensicherheit
- ☐ Telekommunikation und Datenschutz
- ☐ Datenschutz bei Gesundheitsdaten
- ☐ Mitarbeiter- und Bewerberdaten
- ☐ Whistleblowing
- ☐ eigene Schwerpunkte

☐ Ja, Inhouse Schulung ist für uns ein Thema ☐ kontaktieren Sie uns ☐ schicken Sie uns ein Angebot

<Unternehmen/Organisation> <Postleitzahl/Ort/Anschrift>

<Ansprechpartner/Funktion/Abteilung> <Telefon/Fax/Mailadresse>

<Ort/Datum> <Unterschrift>

* Der Reiseaufwand wird individuell kalkuliert und liegt zwischen 400,- und 800,- Euro. Innerhalb Wiens wird pauschaliert EUR 60,- verrechnet.