ARGE DATEN Privacy Austria

Tätigkeitsbericht 2016

ARGE DATEN
www.argedaten.at

Editorial

2016 - der Countdown läuft. Mit Inkrafttreten der Datenschutz-Grundverordnung am 4.5.2016 hat für den europaweiten Datenschutz eine neue Zeitrechnung begonnen. Weniger Bürokratie für Unternehmen, mehr Kompetenzen für die Datenschutzbehörde – das neue Datenschutzrecht verspricht einiges. Eines ist aber klar: Um auf die kommenden Herausforderungen vorbereitet zu sein bedarf es auch einiges an Vorbereitung. Schon jetzt empfiehlt es sich, den notwendigen Handlungsbedarf im Unternehmen zu identifizieren um keine bösen Überraschungen zu erleben.

Die Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr (EU DSGVO) gilt ab 25. Mai 2018.

Sie gilt EU-weit und ersetzt die Richtlinie 95/46/EG. Die Mitgliedstaaten müssen jedoch zu einzelnen Punkten (z.B. Behördenzuständigkeit) nationale Bestimmungen verabschieden. Diese werden in einem eigenen Gesetz für Durchführungsbestimmungen zur EU DSGVO geregelt. Für Österreich ist dieses Gesetz noch ausständig. Jedenfalls gilt bis 25. Mai 2018 das österreichische Datenschutzgesetz (DSG 2000).

Auch Unternehmen außerhalb der EU, insbesondere in den USA, die Daten von EU-Bürgern verarbeiten, müssen sich an die EU-Verordnung halten. Wer die Regelungen bricht, hat mit hohen Strafen zu rechnen.

Verbraucher können neue Rechte wie das Recht auf Vergessenwerden oder das Recht auf Datenportabilität geltend machen. Zusätzlich können Betroffene ihre Beschwerde bei der Datenschutzbehörde ihres Wohnsitzes einbringen, egal in welchem Mitgliedsstaat gegen die EU DSGVO verstoßen wurde.

ARGE DATEN unterstützt Mitglieder

Besonders das in Art. 80 DSGVO normierte Verbandsklagerecht ermöglicht es Betroffenen 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.

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 27. April 2017. 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 2016 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.

Dr. Hans G. Zeger
ARGE DATEN - Privacy Austria

DATENSCHUTZ-STENOGRAMM 2016

OGH (6 Ob 14/16a): Posten eines Fotos auf Facebook ist keine Zustimmung zur Veröffentlichung in Medien

Innenminister Sobotka für Zugriff auf private Überwachungskameras, Kennzeichenerfassung, vorbeugende Fußfesseln und Staatstrojaner

Deutsches Innenministerium veröffentlicht Entwurf für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU

Bodycam für ÖBB-Securitys bei Datenschutzbehörde registriert

EGMR (Barbulescu vs Rumänien): Kontrolle der Internetnutzung am Arbeitsplatz kann mit Art. 8 EMRK vereinbar sein

Hamburger Datenschutzbeauftragter verbietet Facebook Whatsapp-Datenabgleich

Art. 29 Datenschutzgruppe veröffentlicht Leitlinien zur DSGVO (One-Stop-Shop, Recht auf Datenportabilität, Datenschutzbeauftragter)

Datenschutzbehörde schließt Schwerpunktprüfung nach § 30 DSG mit Empfehlungen an Krankenanstalten ab

EuGH (C-582/14): IP-Adressen können personenbezogene Daten sein

„Pokemon Go": Kritik wegen mangelndem Datenschutz

EU-Kommission will Strafhöhe für Spammer drastisch erhöhen

VwGH (9.12.16, Ro 2015/04/0011): Dashcam mit Speichermöglichkeit verstößt gegen DSG 2000

Microsoft muss in Drittstaaten gespeicherte Daten nicht an US-Behörden herausgeben

„Recht auf Vergessenwerden": Französische Datenschutzbehörde verhängt 100.000 EUR Geldstrafe gegen Google

Entwurf der EU-Kommission zur E-Privacy-Verordnung geleaked

EuGH setzt Vorratsdatenspeicherung enge Grenzen (C-203/15 und C-698/15)

ELGA: Rund 255.000 Personen abgemeldet (Stand: November 2016)

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. 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: 25. April 2017
alternativ: 17. Oktober 2017

Modul II:
Datenverwendung im Unternehmen
Termin: 26. April 2017
alternativ: 18. Oktober 2017

Modul III:
Datenschutz und IT-Sicherheit
Termin: 9. Mai 2017
alternativ: 7. November 2017

Modul IV:
Datenschutz EU-Grundverordnung & Praxis
Termin: 27. April 2017
alternativ: 19. Oktober 2017

Modul V:
Datenschutzfragen im Betrieb identifizieren und lösen
(Workshop)
Termin: 10. Mai 2017
alternativ: 8. November 2017

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 2016

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 aber auch Betriebsräte bietet die ARGE DATEN als vertiefende Schulung die Ausbildungsreihe zum „betrieblichen Datenschutzbeauftragten" an.

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

- Verein: Datenschutzrechtliche Ausgestaltung einer Fundraising-Datenbank
- Handelsunternehmen: Kein Kredit nach fehlendem Eintrag bei Wirtschaftsauskunftei
- IT-Unternehmen: Ausgestaltung einer Kundenfrequenzmessung in Einkaufsstraße
- Softwareentwickler: Anforde rungen der DSGVO an Daten banken im Gesundheitsbereich
- Industrieunternehmen: Datenschutzanalyse eines zentralen Mailsystems
- Handelsunternehmen: Arbeitgeberbewertung im Internet
- Konzern: Umgang mit Mitar beiterdaten innerhalb des Konzerns (insb. Binding Corporate Rules)
- Gesundheitsdiensteanbieter: Datenschutzrechtliche Fragen bei Home-Office
- IT-Unternehmen: Cash-Back Kundenbindungsprogramm
- Universität: Protokollierungs vorschriften in der Datenschutz-Grundverordnung
- Handelsunternehmen: Daten schutzrechtliche Einordnung eines Bewerbungsgesprächs per Skype
- Verein: Ausgestaltung einer Zustimmungserklärung im Gesundheitsbereich
- Transportunternehmen: Ein sichtsrechte des Betriebsrats
- Dienstleistungsunternehmen: Meldepflicht im Datenschutzgesetz 2000
- IT-Unternehmen: Pflicht zur Bestellung eines Datenschutzbeauftragten in der Datenschutz-Grundverordnung
- Konzern: Whistleblowing-Hotlines und Datenschutz

Öffentlichkeitsarbeit, Informationsdienst

- Web-Service: rund 43.000 Besucher/Monat
- Newsletter: rund 5.000 Abonnenten
- Medienanfragen/-berichte: rund 500
- Mitgliederbetreuung/ Rechtshilfe: 82 (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:

29% Eingriffe in das Privatleben

28% Betrieb / Beruf / Anstellung

8% Behörden und Verwaltung

7% Finanzdienstleister / Wirtschaftsauskunftsdienste / Privatversicherer

7% Bildung

21% sonstige Anfragen

Veranstaltungen, InHouse Schulungen

65 Personen absolvierten 2016 die ARGE DATEN Ausbildungsreihe zum betrieblichen Datenschutzbeauftragten. Mit rund 530 TeilnehmerInnen waren unsere Datenschutzveranstaltungen sehr gut besucht. Spitzenreiter war die „Jahrestagung Datenschutz 2016" mit 150 Besuchern

Datenschutzthemen 2016
Jahresspiegel Gesetzgebung

EU-Datenschutz-Grundverordnung (DSGVO)

Die Datenschutz-Grundverordnung (DSGVO) tritt mit 25. Mai 2018 in Geltung, gleichzeitig wird die bis dato geltende Datenschutz-Richtlinie 95/46/EG aufgehoben. Mit diesem Tag ist die DSGVO in der gesamten Europäischen Union unmittelbar anwendbar.

Die Mitgliedstaaten haben – trotz unmittelbarer Anwendbarkeit der DSGVO – in gewissen Bereichen die Möglichkeit nähere Bestimmungen zu erlassen bzw. aufrechtzuerhalten. So hat der deutsche Gesetzgeber die Öffnungsklauseln dazu genutzt, den in Deutschland geltenden Bestimmungen zum Datenschutzbeauftragten weiterhin Geltung zu verleihen.

Gesetz für Durchführungsbestimmungen in Österreich noch ausständig

Wann der österreichische Gesetzgeber Fahrt aufnimmt, kann nur schwer abgeschätzt werden. Die ARGE DATEN rechnet mit einem Tätigwerden im Herbst 2017. Der Erlass von Durchführungsbestimmungen zur DSGVO wäre alleine auf Grund einer angemessenen Vorbereitungszeit für verantwortliche Datenverarbeiter dringend geboten.

Die Datenschutz-Grundverordnung kann man als Evolution des Datenschutzrechts beschreiben, keinesfalls als Revolution. Die Grundsätze, die uns aus dem europäischen Datenschutzrecht bekannt sind, bleiben unter dem Versuch, den Herausforderungen des digitalen Zeitalters gerecht zu werden, weitgehend erhalten. Einen Systemwechsel bei der Prüfung der Zulässigkeit von Datenverarbeitungen (Art 6 ff DSGVO), ganz gleich ob es sich um strafrechtsbezogene, sensible oder nichtsensible personenbezogene Daten handelt, wird es nicht geben. Wer die Zulässigkeitsprüfung nach der RL 95/46/EG beherrscht, wird ebenso mit der Zulässigkeitsprüfung der Datenschutz-Grundverordnung wenig Probleme haben.

Auch wenn die Grundsystematik der DSGVO nicht maßgeblich von der RL 95/46/EG abweicht, kann sie doch in einigen Bereichen mit echten Neuerungen aufzeigen. Angesprochen werden muss in diesem Zusammenhang auf die Stärkung der Betroffenenrechte, etwa durch die Einführung eines Rechts auf Datenübertragbarkeit oder eines Rechts auf Einschränkung der Verarbeitung. Diese Betroffenenrechte kannte die RL 95/46/EG nicht.

Neue Pflichten für Unternehmer und Behörden

Völlig neu im Vergleich zum österreichischen Datenschutzrecht sind die Pflichten, die den Auftraggeber (nunmehr „Verantwortlicher“) treffen: Mit dem Wegfall der generellen Meldepflicht von Datenverarbeitungen ist das Datenverarbeitungsregister (DVR) Geschichte. Damit fällt auch die Pflicht zur Führung einer DVR-Nummer weg. Unternehmen haben Datenverarbeitungen künftig in einem Verarbeitungsverzeichnis zu dokumentieren bzw. bei besonders risikoreichen Datenverarbeitungen eine Datenschutz-Folgenabschätzung durchzuführen. Mit dem Datenschutzbeauftragten, der unter gewissen Voraussetzungen verpflichtend zu bestellen ist, wird eines der zentralen Ziele der DSGVO deutlich – den Datenschutz unter mehr Eigenverantwortung im Unternehmen zu etablieren.

Schließlich bedeutet die DSGVO nicht nur für Unternehmen einiges an Anpassungsbedarf. Auch auf die Aufsichtsbehörden der Mitgliedstaaten (in Österreich: Datenschutzbehörde) kommen Neuerungen zu. Neben einem deutlichen Zuwachs an Aufgaben, sind an dieser Stelle die Herausforderungen im Zusammenhang mit der steigenden Kooperation der Aufsichtsbehörden zu erwähnen (Stichwort One-Stop-Shop). Zudem hat die Datenschutzbehörde nunmehr die Kompetenz, Sanktionen zu verhängen, wenn ein Datenverarbeiter oder Auftragsverarbeiter gegen die DSGVO verstößt.

Datenschutz-Richtlinie Polizei und Justiz

Zusammen mit der Datenschutz-Grundverordnung wurde die Datenschutz-Richtlinie für Polizei und Justiz (DSRL-PJ) beschlossen. Im Jahr 2012 wurden die beiden Rechtsakte von der EU-Kommission als Datenschutz-Paket, mit dem Ziel der umfassenden Reformierung des bisher geltenden

Datenschutzrechts, vorgestellt. Die DSRL-PJ löst den Rahmenbeschluss 2008/977/JI ab, den es vor allem auf Grund des sehr engen Anwendungsbereichs zu überarbeiten galt. Während der Rahmenbeschluss auf grenzüberschreitende Datenverarbeitung beschränkt ist, gilt die DSRL-PJ auch für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden auf rein nationaler Ebene. Durch die DSRL-PJ kommt es zu einer (Mindest-)Harmonisierung des Datenschutzniveaus der Mitgliedstaaten bei der Verarbeitung von personenbezogenen Daten durch Justiz- und Polizeibehörden. Der gesetzgeberische Spielraum der Mitgliedstaaten ist jedoch weit. Während nationale Gesetzgeber im Anwendungsbereich der DSGVO bei der Erlassung von Bestimmungen auf „Öffnungsklauseln" beschränkt sind, können die Mitgliedstaaten bezüglich Datenverarbeitungen, die der DSRL-PJ unterliegen, strengere datenschutzrechtliche Bestimmungen als jene der Richtlinie vorsehen (Art 1 Abs 3 DSRL-PJ). Die Bestimmungen der DSRL-PJ müssen bis zum 6. Mai 2018 in nationales Recht umgesetzt werden.

Umbrella Agreement

Mit dem sogenannten „Datenschutz-Rahmenabkommen" (Umbrella Agreement) gelten künftig neue Regeln für den Austausch von personenbezogenen Daten zwischen Polizei und Justiz der USA und der EU. Das Abkommen gilt für alle personenbezogenen Daten (z. B. Namen, Adressen, Strafregisterauszüge), die zwischen der EU und den USA zum Zwecke der Vorbeugung, Aufdeckung, Untersuchung und Verfolgung von Straftaten, einschließlich terroristischer Tätigkeiten, ausgetauscht werden. Betroffenenrechte, wie das Recht auf Information, Auskunft oder Löschung der Daten sind ebenfalls in dem Abkommen vorgesehen. Unklare Formulierungen lassen jedoch nur schwer abschätzen, ob das „Datenschutz-Rahmenabkommen" tatsächlich eine Verbesserung für den Betroffenenschutz bedeutet.

PNR-Richtlinie

Mit der EU-Richtlinie über Fluggastdatensätze (PNR-Richtlinie) wird die Übermittlung von PNR-Daten von Fluggesellschaften an die einzelstaatlichen Behörden sowie die Verarbeitung dieser Daten geregelt. Fluggesellschaften sind verpflichtet, den Behörden der Mitgliedstaaten bei Flügen in die EU oder aus der EU, PNR-Daten zu übermitteln. Darüber hinaus haben die Mitgliedstaaten die Möglichkeit, PNR-Daten für ausgewählte Flüge innerhalb der EU zu erfassen. Die PNR-Daten (PNR=Passenger Name Records) umfassen Informationen wie den Namen des Fluggasts, das Reisedatum, die Reiseroute, Kontaktangaben, die Zahlungsart, die Sitznummer oder Angaben zum Gepäck. Die Daten dürfen ausschließlich zum Zweck der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität verarbeitet werden. Die Richtlinie muss bis zum 25. Mai 2018 in nationales Recht umgesetzt werden.

Die Konformität der PNR-Richtlinie mit der Grundrechtecharta (GRC) muss auf Grund der bisherigen Judikatur des EuGH zur Vorratsdatenspeicherung jedoch bezweifelt werden*. Insbesondere die lange Speicherdauer von fünf Jahren (eine Pseudonymisierung erfolgt nach 6 Monaten) erscheint bedenklich.

Privacy Shield und die EU-Standardvertragsklauseln

Die Safe Harbor-Entscheidung des EuGH war nicht nur der Auslöser für das im Jahr 2016 fertig ausverhandelte „Privacy Shield". Die EU-Kommission war indirekt dazu gezwungen, die bisher geltenden Standardvertragsklauseln einer Überarbeitung zu unterziehen. In einem Beschluss wurden die betroffenen Stellen entsprechend angepasst. Die Auswirkungen auf die Praxis sind aber als gering einzustufen. Die Änderungen beziehen sich nicht auf den Vertragstext selbst, den die Parteien unterzeichnen, sondern auf die Befugnisse der nationalen Datenschutzbehörden. Die Untersagung eines Datentransfers in einen Drittstaat durch eine mitgliedstaatliche Datenschutzbehörde wird nun nicht mehr von bestimmten Voraussetzungen abhängig gemacht, die erfüllt sein müssen, bevor die Befugnis ausgeübt werden kann. Damit wird der Handlungsspielraum der Datenschutzbehörden im Zusammenhang mit Datentransfers in Drittstaaten erweitert.

*Siehe auch Matthias Haller, EU-Fluggastdatensystem und die Grundrechte, SIAK-Journal 2016 H 3, 86.

Der One-Stop-Shop in der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DSGVO) führt den sogenannten One-Stop-Shop ein. Unternehmen müssen bei europaweiten Datenverarbeitungen nur mehr mit einer einzigen Aufsichtsbehörde kommunizieren. Was einen enormen Aufwand und ein hohes Maß an Koordination für die Aufsichtsbehörden bedeutet, soll eine massive Erleichterung für europaweit tätige Unternehmen bringen. Unter der Datenschutzrichtlinie mussten sich Unternehmen mit europaweiten Datenverarbeitungen an viele Datenschutzbehörden wenden.

Damit soll eine zentrale Schwäche des bisherigen europäischen Datenschutzrechts beseitigt werden: Anstatt vieler mitgliedstaatlicher Datenschutzgesetze mit unterschiedlicher Spruchpraxis der Datenschutzbehörden, soll einheitliches Recht uniform ausgelegt werden. In Zukunft werden Aufsichtsbehörden in einem System der Zusammenarbeit und Kohärenz dafür Sorge tragen, dass es zu einer Steigerung der datenschutzrechtlichen Harmonisierung innerhalb der EU kommt.

Eine Aufsichtsbehörde als Ansprechpartner

Das Konzept des One-Stop-Shops (OSS) kommt zur Anwendung, wenn eine „grenzüberschreitende Verarbeitung" personenbezogener Daten vorliegt (Art 56 DSGVO). Zuständig ist dann die sogenannte „federführende Aufsichtsbehörde". Diese ist der einzige Ansprechpartner des Verantwortlichen oder des Auftragsverarbeiters für Fragen bezüglich der grenzüberschreitenden Verarbeitung (Art 56 Abs 6).

Grenzüberschreitende Verarbeitung personenbezogener Daten

Nach Art 4 Nr 23 DSGVO liegt eine grenzüberschreitende Datenverarbeitung vor:
- wenn die Verarbeitung von personenbezogenen Daten im Rahmen der Tätigkeiten von Niederlassungen des Verantwortlichen bzw. Auftragsverarbeiters in mehr als einem Mitgliedstaat erfolgt
- wenn die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen bzw. Auftragsverarbeiters in der Union erfolgt, diese jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann.

Beispiel 1: Die Konzernmutter eines europaweit tätigen Handelsunternehmens hat ihren Sitz in Österreich. Darüber hinaus existieren Tochtergesellschaften in Deutschland und Frankreich. Um geeignete Bewerber für offene Stellen im Konzern zu identifizieren, ist bei der österreichischen Mutter eine Karrieredatenbank eingerichtet. Die konzernweite Karrieredatenbank wird von der jeweiligen Niederlassung genutzt und mit personenbezogenen Daten befüllt (z.B. Qualifikation des Mitarbeiters, Sprachkenntnisse, Dienstzeugnisse und Empfehlungen). Für die Auswertung der Ergebnisse, insbesondere ob ein Mitarbeiter für eine offene Stelle im Konzern geeignet ist, ist der österreichische Standort zuständig. Ergebnis: Es liegt eine grenzüberschreitende Datenverarbeitung im Sinn des Art 4 Nr 23 DSGVO vor, da die Verarbeitung der Mitarbeiterdaten im Rahmen der Tätigkeiten von Niederlassungen des Verantwortlichen in mehr als einem Mitgliedstaat erfolgt. Das OSS-Prinzip kommt für die Datenverarbeitung „Karrieredatenbank" zur Anwendung.

Welche ist die „federführende Aufsichtsbehörde"?

Liegt eine grenzüberschreitende Datenverarbeitung vor, ist grundsätzlich die sogenannte „federführende Aufsichtsbehörde" zuständig. Federführende Aufsichtsbehörde bei der grenzüberschreitenden Datenverarbeitung ist die Aufsichtsbehörde der „Hauptniederlassung" des Verantwortlichen bzw. des Auftragsverarbeiters (Art 56 Abs 1 DSGVO).

Was versteht man unter „Hauptniederlassung"?

Die DSGVO definiert was unter der „Hauptniederlassung" des Verantwortlichen bzw. Auftragsverarbeiters zu verstehen ist. Nach Art 4 Nr 16 ist die Hauptniederlassung im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat prinzipiell mit dessen Hauptverwaltung in der Union gleichzusetzen, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen.

Beispiel 2: Die Konzernmutter des europaweit tätigen Handelsunternehmens hat ihren Sitz in Österreich. Das heißt nicht, dass die „Hauptniederlassung" jedenfalls durch den Ort der Hauptverwaltung der Konzernmutter begründet wird und die österreichische Datenschutzbehörde die federführende Behörde für die Datenverarbeitung „Karrieredatenbank" ist.

Liegt die Entscheidungsbefugnis hinsichtlich der Zwecke und Mittel der Karrieredatenbank bei der (deutschen oder französischen) Zweigniederlassung und ist diese befugt, die Entscheidung umsetzen zu lassen, ist diese Niederlassung die „Hauptniederlassung" im Sinne des Art 4 Nr 16. Die deutsche bzw. französische Behörde wäre die zuständige federführende Aufsichtsbehörde für die konkrete Verarbeitung.

Bei der Bestimmung der Hauptniederlassung ist auf objektive Kriterien abzustellen. Es kommt darauf an, wo die Grundsatzentscheidungen zur Festlegung der Zwecke und Mittel der Verarbeitung getroffen werden. Nicht ausschlaggebend ist, ob die Verarbeitung der personenbezogenen Daten tatsächlich an diesem Ort ausgeführt wird (EG 36).

Hauptniederlassung ist relativ zum Verarbeitungsfall

Der Begriff der „Hauptniederlassung" ist relativ zur jeweiligen Verarbeitungstätigkeit*. Häufig betreiben europaweit tätige Unternehmensgruppen nicht nur eine grenzüberschreitende Datenverarbeitung, sondern mehrere. Um die federführende Behörde für jede dieser grenzüberschreitenden Verarbeitungen bestimmen zu können, muss ermittelt werden, wer über Mittel und Zwecke der jeweiligen Verarbeitung entscheidet. Bei Unternehmen mit Niederlassungen in mehreren Mitgliedstaaten, obliegt die Entscheidungsbefugnis bezüglich der verschiedenen europaweiten Datenverarbeitungen häufig nicht bei einer Niederlassung oder der Hauptverwaltung. Vielmehr werden in den mitgliedstaatlichen Niederlassungen, Entscheidungen über Zwecke und Mittel der grenzüberschreitenden Datenverarbeitungen völlig unabhängig von der Hauptverwaltung getroffen. Ist das der Fall, gibt es innerhalb der Unternehmensgruppe mehrere zuständige federführende Aufsichtsbehörden.

Wie die bisherigen Ausführungen zeigen, dürfte die Bestimmung der Hauptniederlassung in der Praxis nicht immer ganz einfach sein. Die korrekte Bestimmung der federführenden Aufsichtsbehörde ist enorm wichtig. Schließlich hängt davon ab, gegenüber welcher Aufsichtsbehörde die compliance-Pflichten zu erfüllen sind.

Verfahren des OSS im Beschwerdefall

Ein wesentliches Ziel des OSS-Prinzips, neben dem Bürokratieabbau für Unternehmen, ist die Erhöhung des Harmonisierungsgrades der datenschutzrechtlichen Bestimmungen innerhalb der EU. Die alleinige Zuständigkeit der federführenden Aufsichtsbehörde bedeutet nicht, dass diese auch alleine entscheidet. Bei grenzüberschreitenden Datenverarbeitungen wirken alle „betroffenen Aufsichtsbehörden" mit. Das führt im Beschwerdefall dazu, dass alle betroffenen Aufsichtsbehörden und die federführende Aufsichtsbehörde zusammenarbeiten.

Die Ausnahme von der Regel ist Art 56 Abs 2: Jede Aufsichtsbehörde ist dafür zuständig, sich mit einer bei ihr eingereichten Beschwerde oder einem etwaigen Verstoß gegen die Verordnung zu befassen, wenn der Gegenstand nur mit einer Niederlassung in ihrem Mitgliedstaat zusammenhängt oder betroffene Personen nur ihres Mitgliedstaats erheblich beeinträchtigt werden. In jenen Fällen wird das OSS-Prinzip durchbrochen.

„Betroffen" sind die Aufsichtsbehörden
- aller MS, in denen der Verantwortliche/Auftragsverarbeiter niedergelassen ist
- aller MS, in denen Betroffene ihren Wohnsitz haben, auf die die Verarbeitung erhebliche Auswirkungen hat oder haben kann
- bei denen eine Beschwerde eingereicht wurde

Die DSGVO sieht in den Art 60 ff ein Verfahren der Zusammenarbeit der Aufsichtsbehörden vor (Auf Grund der Komplexität des Verfahrens lohnt es sich die Ausführungen in Zusammenschau mit der Grafik zu lesen).

Verfahren der Zusammenarbeit im Beschwerdefall

Wenn sich eine Person in ihren Rechten gemäß der DSGVO verletzt sieht, kann sie Beschwerde bei einer Aufsichtsbehörde (AB) einlegen. Die betroffene Person kann sich u.a. an die Aufsichtsbehörde jenes Mitgliedstaats wenden, indem sie ihren Aufenthalt hat (lokale Aufsichtsbehörde). Nach Art 56 Abs 3 muss die Behörde, bei der die Beschwerde eingebracht wurde, die federführende Behörde konsultieren, wenn sie der Meinung ist, dass es sich um einen „nationalen Fall" nach Art 56 Abs 2 handelt. Ansonsten ist die federführende Behörde zuständig. Diese legt nach Art 60 Abs 3 den anderen betroffenen Aufsichtsbehörden einen Beschlussentwurf zur

*Feiler/Forgo, Kurzkommentar zur EU-Datenschutz-Grundverordnung (2017) Art 56 Rz 2.

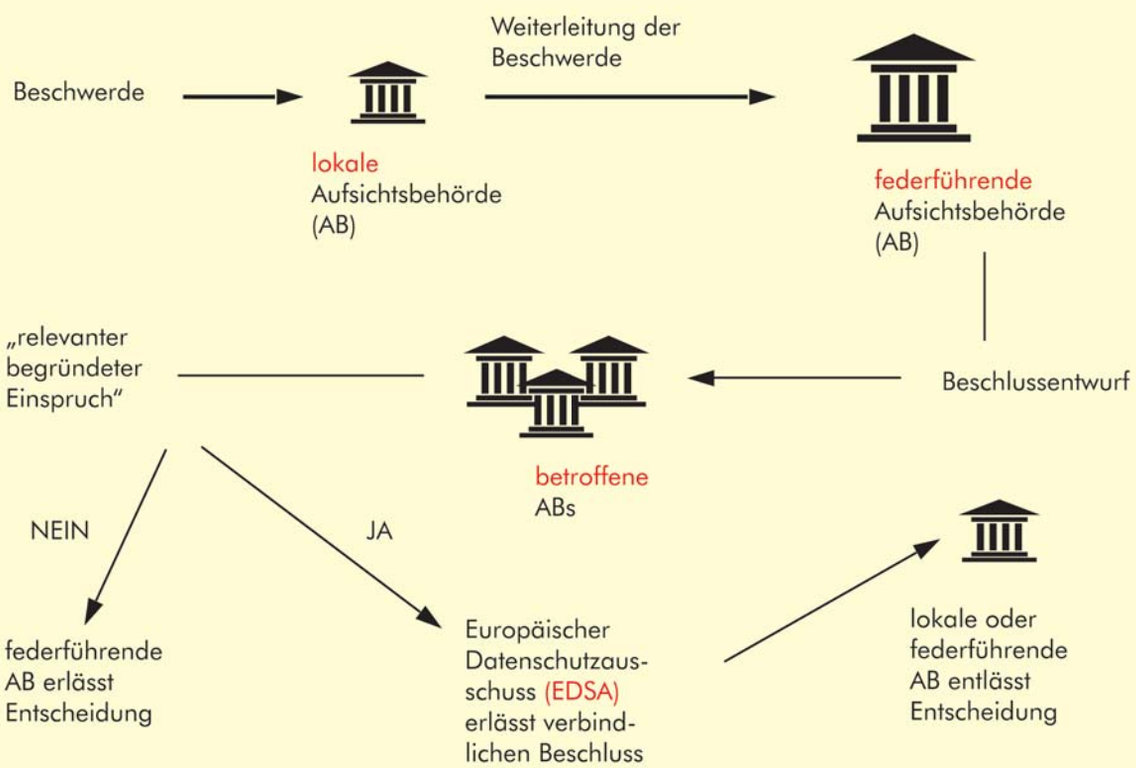
Stellungnahme vor. Eine betroffene Aufsichtsbehörde kann gemäß Abs 4 binnen 4 Wochen einen „maßgeblichen und begründeten Einspruch" (Art 4 Nr 24) gegen den Beschlussentwurf einlegen. Wird kein Einspruch eingebracht, erlässt die federführende Behörde die Entscheidung gemäß dem Beschlussentwurf.

Erfolgt ein Einspruch durch eine betroffene Aufsichtsbehörde und schließt sich die federführende Aufsichtsbehörde dem maßgeblichen und begründeten Einspruch nicht an oder hält sie den Einspruch nicht für maßgeblich und begründet, muss sie das Kohärenzverfahren (Streitbeilegungsverfahren) nach Art 63 iVm 65 DSGVO einleiten. Die federführende

Behörde kann sich dem Einspruch auch anschließen, die betroffenen Aufsichtsbehörden können dann innerhalb einer verkürzten Frist wiederum Einspruch erheben (Art 60 Abs 5).

Nach Einleitung des Streitbeilegungsverfahrens hat der Europäische Datenschutzausschuss (EDSA) innerhalb einer vorgegebenen Frist eine Entscheidung zu erlassen (Art 65 Abs 1). Dieser Beschluss des EDSA ist für die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden bindend (Abs 2). Die endgültige Entscheidung in der Sache wird dem Betroffenen bzw. Verantwortlichen oder dem Auftragsverarbeiter von der zuständigen Aufsichtsbehörde übermittelt. Der Beschluss des EDSA wird der Entscheidung beigefügt und auf der Website des Ausschusses veröffentlicht (Art 65 Abs 6).

Grafik (vereinfachte Darstellung):



Die Datenschutz-Folgenabschätzung

Von der Meldepflicht zur Datenschutz-Folgenabschätzung

Die Abschaffung der generellen Meldepflicht von Datenverarbeitungen kann aus österreichischer Sicht mit Sicherheit als die einschneidenste Neuheit im Datenschutzrecht bezeichnet werden. Bislang waren Datenverarbeitungen bis auf wenige Ausnahmen (z.B. Standardanwendungen) bei der Datenschutzbehörde zu melden.

In anderen Mitgliedstaaten sieht die datenschutzrechtliche Realität anders aus. Schon jetzt entlasten mitgliedstaatliche Datenschutzgesetze, Unternehmen von ihren bürokratischen Pflichten, indem sie weitreichende Ausnahmen von der generellen Meldepflicht normieren. So hat der deutsche Gesetzgeber die Möglichkeiten der Datenschutz-Richtlinie 95/46/EG genutzt und den Entfall der Meldepflicht vorgesehen, wenn die verantwortliche Stelle einen betrieblichen Datenschutzbeauftragten bestellt hat (§ 4d Abs 2 BDSG). Das spart nicht nur Verwaltungsaufwand und -kosten für die Unternehmen, sondern ist auch eine Vorbereitung auf zukünftige Herausforderungen der DSGVO. Eine gleichartige Bestimmung war zwar in der Novelle 2012 zum DSG 2000 vorgesehen, schaffte es aber nicht in das Gesetz. Die Datenschutz-Grundverordnung sieht die Rolle des Datenschutzbeauftragten neben der Pflicht zur Führung eines Verfahrensverzeichnisses als Ersatz für die behördliche Meldepflicht an.

Auch die Vorabkontrolle von sensiblen Datenverarbeitungen durch die Datenschutzbehörde wird es in der Form nicht mehr geben. Als Äquivalent müssen Unternehmen gemäß der DSGVO in gewissen Fällen vor Aufnahme der Verarbeitungstätigkeit eine Datenschutz-Folgenabschätzung durchführen. Der Gesetzestext rückt an dieser Stelle den Risikobegriff in den Vordergrund. Gemeint sind die potentiellen Auswirkungen, die eine Verarbeitungstätigkeit auf die Rechte und Freiheiten eines Menschen haben kann. Der Risikoansatz der Datenschutz-Grundverordnung darf nicht mit dem unternehmerischen Risikomanagement verwechselt werden. Die Prinzipien des Risikoansatzes im Datenschutz unterscheiden sich schon hinsichtlich der Zielsetzung grundlegend von den Prinzipien des Risikomanagements. Datenschutz will negative Auswirkungen, die eine Verarbeitungstätigkeit auf die Rechte und Freiheiten eines Menschen haben kann, möglichst ausschalten. Der Betroffene steht im Zentrum, ist Schutzobjekt. Hingegen ist beim Risikomanagement das Risiko für eine Organisation und die unternehmerische Tätigkeit im Fokus.

Wann ist eine DSFA durchzuführen?

Nach Art 35 DSGVO muss der Verantwortliche bei Formen der Verarbeitung, insbesondere bei Verwendung neuer Technologien, die aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen. Die Datenschutz-Folgenabschätzung ist vor der Aufnahme der Datenverarbeitung vorzunehmen.

Die DSGVO nennt in Art 35 Abs 3 Beispiele, in denen eine Datenschutz-Folgenabschätzung jedenfalls durchzuführen ist. Welche Datenverarbeitungen darüber hinaus ein hohes Risiko zur Folge haben, ist schwer zu bestimmen, da die DSGVO nur sehr wenige Anhaltspunkte bietet. Eine wesentliche Rolle haben in diesem Zusammenhang die Aufsichtsbehörden der Mitgliedstaaten. Die Aufsichtsbehörde erstellt nach Art 35 Abs 4 eine Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese („schwarze Liste"). Nach Abs 5 kann die Aufsichtsbehörde des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist („weiße Liste"). Eine von der österreichischen Datenschutzbehörde erstellte weiße Liste könnte sich an der derzeit in Geltung stehenden Standard- und Muster-Verordnung (StMV 2004) orientieren. Der Entwurf einer schwarzen oder weißen Liste ist zwar dem Europäischem Datenschutzausschuss (EDSA) zur Stellungnahme vorzulegen (Art 64 Abs 1 lit a), das Kohärenzverfahren kommt jedoch nur zur Anwendung, wenn die Datenverarbeitung einen gewissen unionsrechtlichen Bezug aufweist (Art 35 Abs 6). Das Ergebnis ist, dass es in der EU keine einheitliche schwarze oder weiße Liste geben wird, sondern in den Mitgliedstaaten unterschiedliche schwarze und weiße Listen existieren werden. Damit wird dem Gedanken der Harmonisierung der DSGVO nicht entsprochen.

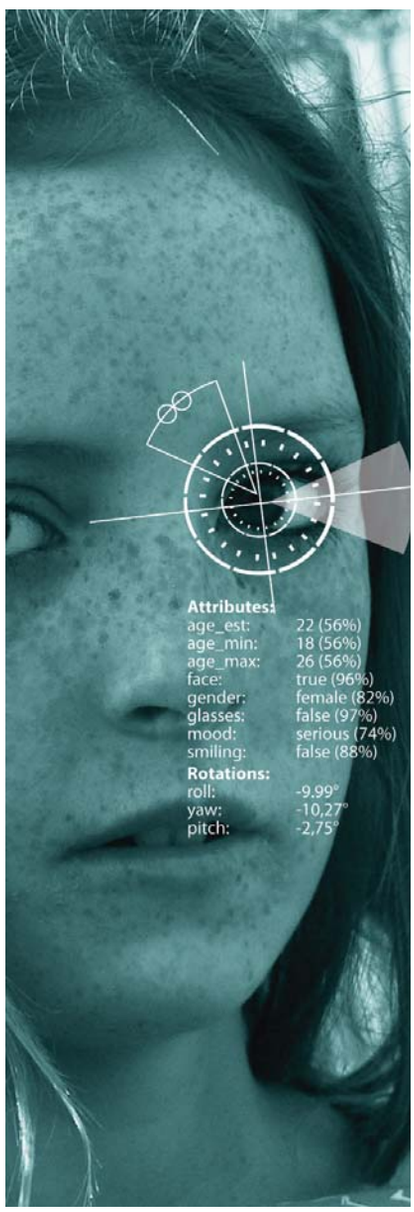
Inhalt der DSFA

In Art 35 Abs 7 gibt die Datenschutz-Grundverordnung lediglich einen Mindestinhalt vor. Darunter kann keinesfalls eine Anleitung zur Durchführung einer Datenschutz-Folgenabschätzung verstanden werden. Welche zusätzlichen inhaltlichen und organisatorischen Schritte für eine umfassende Risikoabschätzung durchzuführen sind, wird die Rechtspraxis zeigen. Die Evaluierung der Risiken für die Rechte und Freiheiten der betroffenen Personen muss jedenfalls so ausgestaltet sein, dass diese eine valide Grundlage für die Planung und Implementierung von Abhilfemaßnahmen bietet. Für einen ersten Überblick zur Thematik der Datenschutz-Folgenabschätzung und wie diese in der Praxis durchgeführt werden kann, lohnt sich die Auseinandersetzung mit zwei Empfehlungen der EU-Kommission. Trotz fehlender Pflicht in der DSRL 95/46 erließ die EU-Kommission Empfehlungen zu Datenschutz-Folgenabschätzung im Zusammenhang mit RFID-Anwendungen und Smart Meters.

Vorherige Konsultation der Aufsichtsbehörde

Auch wenn die allgemeine Meldepflicht abgeschafft wird, muss die Datenverarbeitung unter Umständen nach Durchführung einer Datenschutz-Folgenabschätzung bei der Datenschutzbehörde gemeldet werden. Geht aus der Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung ein hohes Risiko zur Folge hätte und kann dieses Risiko nicht durch (auch im Hinblick auf Implementierungskosten) verfügbare Mittel eingedämmt werden, muss die Aufsichtsbehörde konsultiert werden (Art 36 Abs 1). Diese erteilt dann gegebenenfalls Empfehlungen.

Der Wortlaut des Art 36 Abs 1 lässt den Schluss zu, dass der Verantwortliche die Reaktion der Aufsichtsbehörde nicht abwarten muss, bevor er mit der Datenverarbeitung beginnt. Somit besteht zwar eine Pflicht, die Konsultierung einzuleiten, abgeschlossen muss das Konsultationsverfahren aber nicht sein*.



Die Videoüberwachung in der DSGVO

Die ARGE Daten erhält seit der Veröffentlichung des finalen Texts der Datenschutz-Grundverordnung (DSGVO) laufend Anfragen zur Thematik der Videoüberwachung. Offenbar bedingt durch das Ziehen voreiliger Schlüsse - den Begriff „Videoüberwachung" findet man lediglich in einem Erwägungsgrund - besteht vielfach die Annahme, dass der Einsatz von Videoüberwachung ab der Gültigkeit der DSGVO ohne Einschränkung möglich sei. Ein Trugschluss, der ab dem Frühsommer 2018 schwerwiegende (finanzielle) Konsequenzen haben kann. Auch wenn viele Fragen nach wie vor offen sind, ist es notwendig, sich schon jetzt mit den Bestimmungen der DSGVO auseinanderzusetzen, um böse Überraschungen zu vermeiden. Wenn die Bestimmungen des DSG 2000 zur Videoüberwachung vom österreichischen Gesetzgeber nicht ohnehin aufgehoben werden, sind sie spätestens mit dem Wirksamwerden der DSGVO nicht mehr anwendbar.

Videoüberwachung morgen (DSGVO)

Explizite Bestimmungen zur Videoüberwachung sucht man in der Datenschutz-Grundverordnung vergeblich, Spezialbestimmungen wie im DSG 2000 gibt es keine. Heißt das, dass es ab dem 25. Mai 2018 keine Einschränkungen beim Einsatz von Videoüberwachungen geben wird? Keineswegs. Vorbehaltlich der Einordnung von Videodaten als nicht-sensible Daten (die Gretchenfrage ist noch immer nicht vollends geklärt) gilt Folgendes:

*Feiler/Forgo, Kurzkommentar zur EU-Datenschutz-Grundverordnung (2017) Art 36 Rz 2.

Die DSGVO normiert in Art 5 die Grundsätze, die bei jeder Datenverarbeitung eingehalten werden müssen - auch bei der Videoüberwachung. So muss die Datenverarbeitung rechtmäßig sein (Art 5 Abs 1 lit a). Maßgeblich für die Rechtmäßigkeit der Videoüberwachung im privaten Bereich ist zunächst die Generalklausel des Art 6 Abs 1 lit f. Danach ist die Verarbeitung rechtmäßig, wenn sie „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich sind, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt." Es ist also eine Interessenabwägung durchzuführen, die uns auch schon aus dem DSG 2000 bekannt ist. Im Gegensatz zum DSG 2000 fordert die DSGVO zu einer besonders sorgfältigen Abwägung auf, wenn vermehrt Kinder den erfassten Bereich durchschreiten oder sich in diesem aufhalten.

Denkbar ist der rechtmäßige Einsatz einer Videoüberwachung beispielsweise auch, wenn dies zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist (lit d) oder um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen (lit d).

Wie bei jeder Datenverarbeitung muss auch bei der Videoüberwachung der Grundsatz der Zweckbindung eingehalten werden. Gemäß Art 5 Abs lit b „müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden". Die DSGVO gibt die Zwecke, anders als das DSG 2000 nicht vor.

Schließlich muss der Verhältnismäßigkeitsgrundsatz beachtet werden. Die Videoüberwachung darf nur eingesetzt werden, wenn kein gelinderes Mittel eingesetzt werden könnte.

Führt der Entfall der Meldepflicht zu neuen Pflichten?

Auch wenn die generelle Meldepflicht von Datenverarbeitungen mit der DSGVO entfällt, muss die Videoüberwachung entsprechend dokumentiert werden. Nach Art 30 DSGVO hat jeder Verantwortliche ein Verfahrensverzeichnis zu erstellen. In das Verfahrensverzeichnis sind neben den einzelnen installierten Videokameras, u. a. der Zweck der Verarbeitung, Löschungsfristen und eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus nach Art 32 aufzunehmen.

Bei einer Videoüberwachung, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, muss der Verantwortliche darüber hinaus eine Datenschutz-Folgenabschätzung durchführen.

Verdeckte Videoüberwachung

Das DSG 2000 normiert im Gegensatz zur DSGVO ausdrücklich die Pflicht zur Kennzeichnung einer Videoüberwachung, die nur bei Vollziehung hoheitlicher Aufgaben nicht erfüllt werden muss. Dies gilt auf Grund von § 50d DSG sogar, wenn der Verdacht einer strafbaren Handlung durch einen Mitarbeiter besteht, obwohl dies aus verfassungsrechtlicher Sicht nach einem Urteil des Europäischen Gerichtshof für Menschenrechte (EGMR) zu Art 8 EMRK, nicht unbedingt geboten ist (5.10.2010, 420/07, Karin Köpke). In dieser Entscheidung hatte der EGMR die zweiwöchige Installation einer verdeckten Videoüberwachung - im konkreten Fall - als verhältnismäßig erachtet.

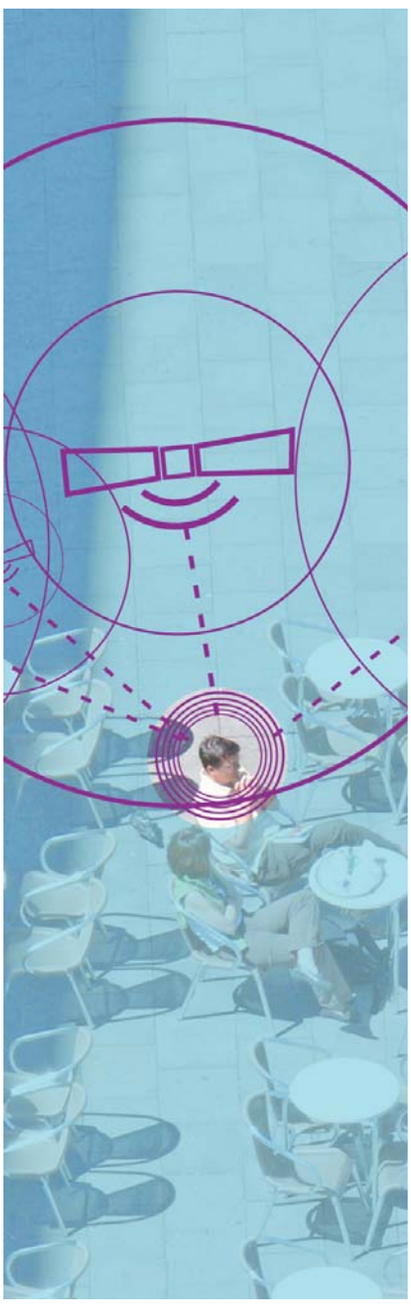
In diesem Sinn hat auch das deutsche Bundesarbeitsgericht eine verdeckte Videoüberwachung eines Mitarbeiters mangels verbleibender Mittel als nicht unverhältnismäßig erachtet (21.06.2012, 2 AZR/153/11). Die Urteile zeigen, dass eine verdeckte Videoüberwachung mit dem europäischen Grundrechteverständnis durchaus vereinbar sein kann, wenn auch in sehr beschränktem Maße.

Eines steht aber fest: Obwohl nicht explizit genannt, wird die Kennzeichnungspflicht von Videoüberwachungen mit der DSGVO bestehen bleiben. Die Pflicht, Betroffene von der Videoüberwachung zu informieren, ist aus Art 13 DSGVO ableitbar (Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person). Den Mitgliedstaaten steht offen, die Informationspflicht zu beschränken, sofern dies zur Sicherstellung der in Art 23 festgelegten Interessen notwendig ist (z.B. zum Schutz der betroffenen Person).

Videoüberwachung zur Mitarbeiterkontrolle

§ 50a Abs 5 DSG 2000 bestimmt explizit, dass die Videoüberwachung zum Zweck der Mitarbeiterkontrolle an Arbeitsstätten untersagt ist. Auch wenn die DSGVO ein gleichartiges Verbot nicht

kennt, wird die Mitarbeiterüberwachung zur Leistungskontrolle auch künftig nicht zulässig sein. Auf Grund des massiven Grundrechtseingriffs ist davon auszugehen, dass stets ein gelinderes Mittel zur Kontrolle von Mitarbeitern angewandt werden kann. Nichtsdestotrotz könnte der österreichische Gesetzgeber über die Öffnungsklausel in Art 88 DSGVO (Beschäftigtendatenschutz) ein Verbot der Mitarbeiterkontrolle auch ausdrücklich vorsehen.



Privacy Shield – Rechtssicherheit für Datentransfers in die USA?

Hintergrund

Mit Privacy Shield hat die EU-Kommission jene Lücke geschlossen, die sich mit dem Schrems-Urteil des EuGH aufgetan hatte. Nach der Aufhebung von Safe Harbor waren viele Datentransfers in die USA schlagartig genehmigungspflichtig geworden. Da ein möglichst reibungsloser Datenverkehr zwischen der EU und den USA von großer Bedeutung für die transatlantischen Wirtschaftsbeziehungen ist, musste schnell eine Lösung gefunden werden. Mit Privacy Shield wurden die Grundsätze von Safe Harbor weiterentwickelt. Ob das „Datenschutzschild" die Vorgaben, die der EuGH in der Rechtssache C-362/14 gemacht hat, erfüllen kann, wird von der ARGE Daten angesichts der weiterhin gültigen Gesetze zur Massenüberwachung in den USA bezweifelt.

Zustandekommen und Bedeutung

Auf der Grundlage von - teilweise in Briefform gegebenen - Zusicherungen seitens der US-Regierung und US-Behörden erließ die EU-Kommission im Juli 2016 die Angemessenheitsentscheidung C(2016) 4176 final, kurz „Privacy Shield".

US-Unternehmen, die sich den Prinzipien von Privacy Shield unterwerfen, wird ein angemessenes Datenschutzniveau attestiert. Personenbezogene Daten aus den EU-Mitgliedstaaten (und den drei EWR-Mitgliedern Norwegen, Liechtenstein und Island) können an selbstzertifizierte US-Unternehmen ohne Genehmigung durch die Datenschutzbehörde transferiert werden.

Eine Zertifizierung ist seit dem 1. August 2016 beim US-Department of Commerce möglich. Die Liste der zertifizierten Unternehmen kann unter https://www.privacyshield.gov/welcome abgerufen werden. Anfang 2017 sind rund 500 Unternehmen zertifiziert und in der Liste eingetragen. Darunter eine Vielzahl der großen amerikanischen Internet- und Cloudanbieter.

Selbstzertifizierung – Privacy-Shield-Prinzipien

Um sich auf Privacy Shield stützen zu können, müssen sich US-Unternehmen im Wege der Selbstzertifizierung verpflichten, die vom Department of Commerce festgelegten Prinzipien (z.B. Auskunftspflicht) einzuhalten. Die Prinzipien entsprechen weitgehend jenen von Safe Harbor, sind aber teilweise konkreter gefasst. Die Selbstzertifizierung ist jährlich zu wiederholen.

Darüber hinaus sind Unternehmen verpflichtet eine Datenschutzrichtlinie zu veröffentlichen, die mit den Prinzipien im Einklang steht. Das Department of Commerce muss Unternehmen, die dauernd gegen die Prinzipien verstoßen oder die Zertifizierung nicht erneuern, von der Privacy Shield-Liste streichen. Gestrichene Unternehmen werden in eine eigene Liste eingetragen, die ebenfalls öffentlich abrufbar ist.

Beschwerdemöglichkeiten für Betroffene

Insgesamt kann man – zumindest auf dem Papier - von einer Stärkung des Rechtsschutzes für europäische Bürger durch Privacy Shield sprechen.

Die Regelungen können zwar nicht als verbraucherfreundlich

bezeichnet werden, da sie kompliziert ausgestaltet sind. Zumindest haben Betroffene, die einen Missbrauch ihrer personenbezogenen Daten vermuten, durch Privacy Shield mehrere Möglichkeiten eine Beschwerde einzulegen. An welche Stelle die Betroffenen ihre Beschwerde richten müssen, hängt davon ab, ob sich das US-Unternehmen zu einer alternativen Streitbeilegung verpflichtet hat oder nicht. Bürger können sich jedenfalls an die Datenschutzbehörden der Mitgliedstaaten wenden, die zusammen mit der Federal Trade Comission (FTC) für Abhilfe sorgen sollen. Das letzte Mittel stellt ein Schiedsverfahren dar. Für Beschwerden, die sich gegen Überwachungsmaßnahmen richtet, ist ein Ombudsmann zuständig. Dieser berichtet unmittelbar dem Außenministerium und ist unabhängig von den Geheimdiensten.

Ob es tatsächlich zu merkbaren Verbesserungen für Betroffene kommt, wird erst die Praxis zeigen. Betroffene sind weitgehend vom Handeln oder eben Nicht-Handeln der US-Behörden abhängig, was zu massiven Rechtsschutzdefiziten führen kann. Insgesamt ist daher zu befürchten, dass das Schutzniveau für Betroffene trotz Verbesserungen auf dem Papier deutlich hinter dem europäischen Standard zurückbleiben wird.

Besserer Schutz für Mitarbeiterdaten?

Tatsächlich zu merkbaren Verbesserungen könnte es hinsichtlich des Schutzes personenbezogener Mitarbeiterdaten kommen. Durch die Privacy-Shield-Prinzipien sind US-Unternehmen verpflichtet sich der jeweils zuständigen europäischen Datenschutzbehörde direkt zu unterwerfen, wenn personenbezogene Mitarbeiterdaten an diese transferiert werden. Zumindest hinsichtlich des Arbeitnehmerdatenschutzes kann man also von einem Fortschritt im Vergleich zur Vorgängerregelung sprechen.

Mehr Rechtssicherheit für Unternehmen?

Ob Privacy Shield dauerhafte Rechtssicherheit für Unternehmen bringt, muss bezweifelt werden. Privacy Shield wird jährlich von der EU-Kommission und vom US-Department of Commerce überprüft. Kriterium wird insbesondere sein, ob die Zusicherung der Einschränkung des Zugriffs auf personenbezogene Daten von EU-Bürgern durch US-Behörden auch tatsächlich eingehalten wird. Entspricht das Schild nicht den Anforderungen, können die Bestimmungen ausgesetzt werden.

Seit dem Jahresende prüft eine weitere EU-Institution. Auf Grund massiver Kritik war es nur eine Frage der Zeit bis sich der Europäische Gerichtshof (in diesem Fall das Europäische Gericht) mit Privacy Shield beschäftigen muss. Die Klägerin Digital Rights Ireland Ltd beantragt in ihrer Klage, Nichtigerklärung und Aufhebung von Privacy Shield durch den EuG. Nach der Prüfung der Zulässigkeit der Klage, muss sich der EuG mit der Begründetheit der Klage auseinandersetzen. Die Erfolgsaussichten können derzeit nicht abgeschätzt werden. Mit einem Urteil ist frühestens Ende 2017 zu rechnen.

Fazit

Privacy Shield bietet nur eingeschränkt Rechtssicherheit für Unternehmen mit Datenfluss in die USA. Für Unternehmen lohnt es sich daher, die Datenübermittlung oder –überlassung zusätzlich auf Standardvertragsklauseln zu stützen, um im Falle der Aussetzung oder Aufhebung von Privacy Shield nicht ohne Rechtsgrundlage dazustehen.

Ein sicherer und nicht genehmigungspflichtiger Weg ist die Datenübermittlung oder –überlassung innerhalb der EU. Der Datenverkehr innerhalb der EU unterliegt nicht der Genehmigungspflicht durch die Datenschutzbehörde. Betroffenen kommt außerdem der vergleichsweise starke mitgliedstaatliche Rechtsschutz zu Gute.

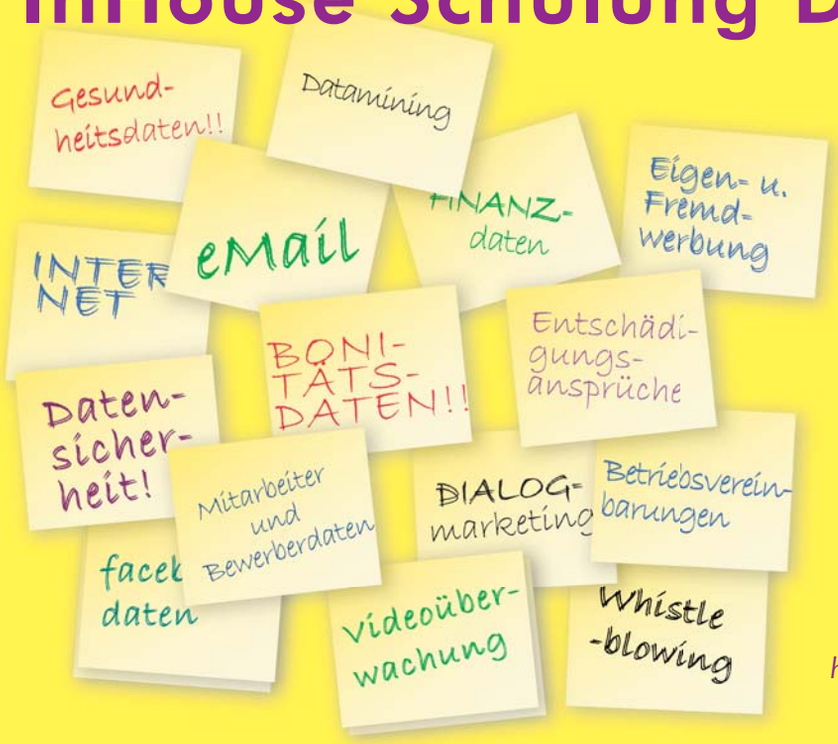
Impressum:

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: Mag. jur. 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.