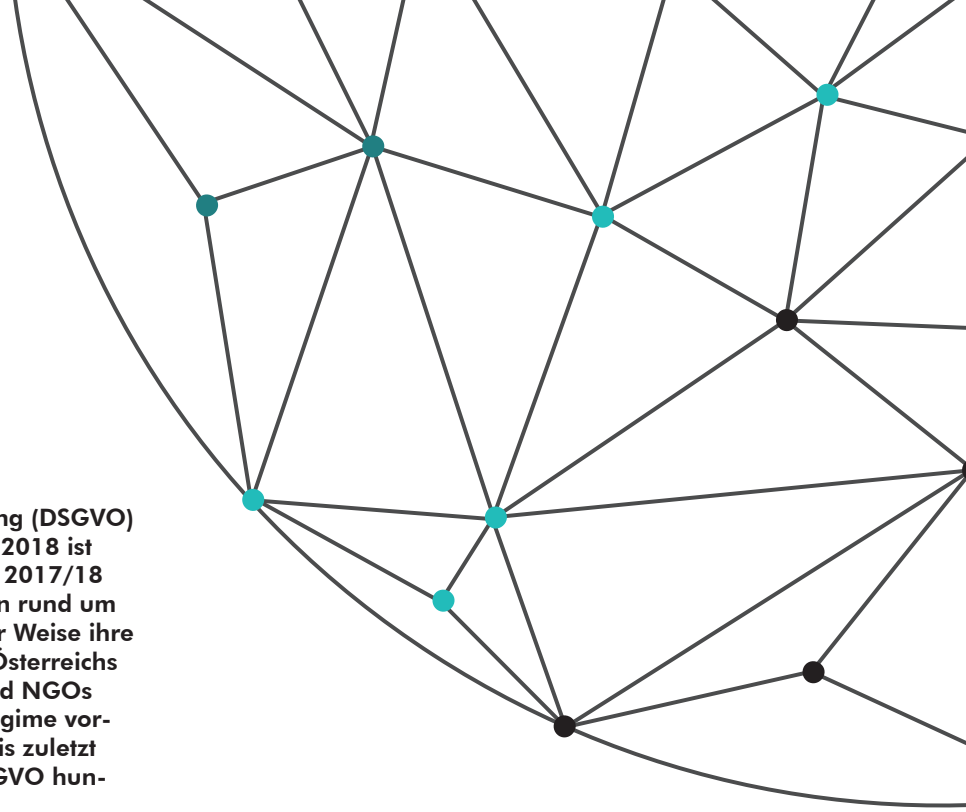
PRIVACY AUSTRIA TÄTIGKEITSBERICHT 2017/18

ARGE DATEN

http://www.argedaten.at/



EDITORIAL

2016 Beschluss der Datenschutzgrundverordnung (DSGVO) - 2017 das Jahr der Vorbereitung zur DSGVO - 2018 ist die DSGVO anzuwenden - der Tätigkeitsbericht 2017/18 steht ganz im Zeichen praktischer Informationen rund um die DSGVO - die ARGE DATEN hat in vielfältiger Weise ihre Mitglieder in den Vorbereitungen unterstützt - Österreichs Unternehmen, aber auch zahlreiche Vereine und NGOs haben sich intensiv auf das neue Datenschutzregime vorbereitet - nicht so Österreichs Politik - säumig bis zuletzt wurden erst ein Monat vor Anwendung der DSGVO hunderte Gesetze geändert.

SCHAFFT EUROPA MIT DER DSGVO DEN ANSCHLUSS AN DIE INFORMATIONSGESELLSCHAFT?

Wir erleben in den letzten Jahren eine rasante Entwicklung der globalen Automatisierung von Geschäftsprozessen. Davon sind zwar alle Lebensbereiche betroffen, doch nur wenige haben zeitgerecht begonnen die ausreichenden Rahmenbedingungen zu schaffen.

„Control" ist das Zauberwort, „steuern" statt verwalten ist der Anspruch aktueller Prozess-Informatik. Österreichs Verwaltung, besonders die öffentliche und staatsnahe, arbeitet mit Informationstechnik noch immer auf einem Niveau der 70er Jahre. Informationstechnik soll bestehende Abläufe unterstützen und erleichtern (Verwaltungs-Informatik). Viele glauben, der Einsatz von eMail, Excel-Tabelle, Filesharing und Smartphone sind modern, ein Irrglaube, der uns immer weiter weg vom IT-Weltniveau bringt.

Im Zeitalter der Verwaltungs-Informatik war die Idee vom „Datenschutz" ein Abwehrrecht gegen unverstandene Technik und gefährliche Technokraten, eine Art Maschinenstürmer-Lizenz. Abgehandelt wurde das Thema aus Konsumentensicht, Unterkategorie „Opfer".

Damit will die DSGVO aufräumen. Was will eigentlich die DSGVO? Der Anspruch ist simpel, „Organisationen sind verpflichtet Informationsprozesse grundrechtskonform zu gestalten".

IN DIESER ANFORDERUNG STECKEN DREI BOTSCHAFTEN:

a. die Organisationen müssen wissen, welche Prozesse bei ihnen überhaupt stattfinden,
b. die Organisationen haben diese Prozesse zu gestalten,
c. die Grundrechte auf Privatsphäre sind in Einklang mit den Prozessen zu bringen.

Im Rahmen der DSGVO-Umsetzung wurden in den letzten Monaten hunderte Gespräche geführt. In vielen Fällen war das ernüchternde Ergebnis, dass die Basics, die Voraussetzungen „Wissen über die eigenen Prozesse" und „Gestaltung" in vielen Organisationen nicht gegeben waren.
An eine grundrechtskonforme Umsetzung war gar nicht zu denken.

Das historische Beispiel des Buchdrucks der 80er-Jahre sollte zu denken geben. Aus der klassischen Wertschöpfungskette Autor -> Verleger/Lektor -> Setzer -> Drucker -> Buchhändler -> Konsument wurde Autor -> Konsument. Und in vielen Fällen nicht einmal mehr das, wenn wir an Wikipedia und Co denken, wo Konsumenten für Konsumenten produzieren und ein gesamter Wertschöpfungsbereich wegfällt.

Ein weiteres Beispiel ist der Uber/Taxi-Konflikt. Wer glaubt, per Telefon in einer Taxizentrale anzurufen, die dortige Mitarbeiterin ruft per Funk die Bestellung aus und der am schnellsten drückende Taxifahrer übernimmt den Call, das sei modern, sollte sich in eine Zeitmaschine setzen und sich in die (IT-)Steinzeit beamen lassen.

In Zeiten von Navi, Smartphone, Apps und Carsharing sind Taxizentralen, Funksysteme, Taxlerausbildung und Taxireglementierungen bestenfalls hilflose Versuche geschützte Werkstätten zu erhalten. Es wird für Sie nur ein kleiner Trost sein, Uber ist noch lange nicht das Ende der Fahnenstange, hier sind noch viel weitergehende Automationsprozesse möglich.

Damit in diesem System der automatisierten Entscheidungsfindung - nichts anderes ist das Taxi-System der Zukunft - nicht die Konsumenten unter die Räder kommen, braucht es eine grundrechtskonforme Gestaltung der Prozesse. Dieser Aufgabe verweigert sich jedoch Österreichs Politik und hofft Uber und Co werden schon wieder verschwinden, ähnlich wie ja die Eisenbahn nach ihrem Erscheinen im 19. Jahrhundert verschwunden ist.

Wie darauf reagieren? Meist wird versucht einzelne Phänomene der Prozess-Informatik zu kriminalisieren oder zumindest bürokratisch zu erschlagen. Verbot von Uber und Airbnb, neue Digitalsteuern, Verbot der Privatvermietung, ...
Eine Alternative wäre jedoch Prozess-Informatik grundrechts-

konform zu organisieren. Wird dieser Anspruch umgesetzt, kann er auch von anderen Betreibern eingefordert und durchgesetzt werden. Dann wären EU-Uber, EU-Airbnb und EU-Google ein Teil der Lösung.

Österreichs Politik in der Informationstechnik beschränkt sich auf das Verwalten der Konsumentenrolle. Es stimmt bedenklich, wenn das zugehörige Ministerium „für Digitalisierung" heißt und sich mit der Installation von Breitband, verteilen von Tablets und Verbilligen von Smartphone-Tarifen beschäftigt. Wichtige Konsumenten-Angelegenheiten gewiss, doch gehen sie an den heutigen Herausforderungen vorbei.

Wir erleben eine dramatische Komprimierung von Arbeitsprozessen. Sie können heute eine global agierende Full-Service-Bank mit wenigen 100 Mitarbeitern führen (siehe N26). Wie viele Mitarbeiter haben Österreichs führende Bank-Institute? Mit „natürlichem" Abgang wird der Übergang in die neue Zeit nicht zu schaffen sein.

„BigData" soll das neue Gold des Informationszeitalters sein. Wer daran glaubt, sollte sich vergegenwärtigen, dass die Goldquote abbauwürdiger Lagerstätten bei weniger als 0,01 Promille liegt (bei etwa 10 ppm). Die Bergbauindustrie musste hochkomplexe Technologien entwickeln, um bei dieser Quote noch kostendeckend arbeiten zu können.

Im Data-Bereich wird die Schürf-Quote noch wesentlich darunterliegen, die diesbezüglich notwendigen Qualifikationen und Kompetenzen werden in Österreich nicht einmal diskutiert, geschweige denn vermittelt.

Analytik, Logik, Heuristik, aber auch Rhetorik sind die Kernkompetenzen der Zukunft. Niemand wird dafür bezahlt werden, dass er ein Smartphone bedienen kann. Genauso wenig, wie jemand zum Politiker wird, wenn er sich besonders viele Folgen von „House of Cards" ansieht.

Mit der Konsequenz, dass die Tracking-, Targeting- und Nudging-Industrie für Europa verloren ist. Europäer sind hier nur mehr Ziel, Betroffene, „Opfer".
Die DSGVO - richtig angewandt - wäre eine Gelegenheit, Versäumnisse der letzten Jahrzehnte aufzuholen. Sie könnte uns zwingen IT-Prozesse endlich zu gestalten, statt sich ihnen bloß wie Konsumenten zu unterwerfen.

Die letzten Monate haben mich jedoch skeptisch gemacht. Das offizielle Österreich jubelt, dass Grundrechtsverletzungen straffrei bleiben sollen, dass man kritische IT-Prozesse keiner Risiko-Analyse unterziehen muss und dass Informationsrechte der Bürger eingeschränkt werden dürfen.

„Glück gehabt, wir können weitermachen wie bisher", erlebe ich als Reaktion bei vielen Verantwortlichen. Ich fürchte außer den großen US-Unternehmen sind wenige Unternehmen auf die neue DSGVO gut vorbereitet.

GLOBAL GESEHEN STEHEN HEUTE DREI GESELLSCHAFTSSYSTEME AUF DEM PRÜFSTAND.

Erstens, das System der „Citizen Society" der USA. Der US-Bürger, also alle USA-Staatsbürger weltweit und alle legal in den USA aufhältigen Bürger, genießen besonderen Schutz, besondere Rechte aber hat auch besondere Pflichten, wie etwa beim Steuerzahlen.

Zweitens, das System der „Civil Rights Society" der EU. Alle Bürger weltweit sind gleich in Rechten und Pflichten und alle Staaten haben sich um mögliche Opfer des (Wirtschafts-)Systems zu kümmern.

Drittens, das System der „Social Profiling Society" von China. Rechte und Pflichten der Bürger leiten sich aus der lebenslangen Bewertung seines individuellen Verhaltens ab.

Das anspruchsvollste System ist wohl das der EU, es kann jedoch nur durch hohe Selbstdisziplin der Menschen funktionieren. Selbstdisziplin sowohl was die Bereitschaft zur Änderung und Anpassung an neu Prozesse betrifft, als auch in der Beschränkung wer als Opfer anzusehen ist. Streben alle die Opferrolle an, wird ein derartiges System unfinanzierbar. Aber vielleicht ist die Vorstellung einer Menschenrechts-Gesellschaft eine Illusion, vergleichbar den kommunistischen und sozialistischen Gesellschaften des 20. Jahrhunderts.

Dr. Hans G. Zeger
Obman ARGE DATEN - Privacy Austria

ARGE DATEN

AUSBILDUNGSREIHE „BETRIEBLICHER DATEN-SCHUTZBEAUFTRAGTER“

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

WARUM „BETRIEBLICHER DATENSCHUTZBEAUFTRAGTER“?

Der betriebliche Datenschutzbeauftragte ist eine der wichtigsten Neuerungen der Datenschutz-Grundverordnung (DSGVO).

Ab 25. Mai 2018 sind ALLE Behörden und öffentlichen Stellen verpflichtet einen Datenschutzbeauftragten zu haben. Unternehmen, deren Haupttätigkeit in der „umfangreichen regelmäßigen und systematischen Überwachung von betroffenen Personen“ oder in der „umfangreichen Verarbeitung von sensiblen oder strafrechtlich relevanten Daten“ besteht, müssen ebenfalls einen Datenschutzbeauftragten bestellen (Art 39 Abs 1 lit b und c). Alle anderen Unternehmen können freiwillig einen Datenschutzbeauftragten bestellen.

Die Aufgaben, die dem Datenschutzbeauftragten von der Datenschutz-Grundverordnung übertragen werden, sind vielfältig: Nach Art 39 DSGVO unterrichtet der Datenschutzbeauftragte die Geschäftsleitung und Mitarbeiter über ihre datenschutzrechtlichen Pflichten. Gleichzeitig hat er die Einhaltung der Verordnung zu überwachen und ist Anlaufstelle für die Aufsichtsbehörde. Weiters berät der Datenschutzbeauftragte im Zusammenhang mit der Durchführung einer Datenschutz-Folgenabschätzung.

Über diese Aufgaben hinaus können dem Datenschutzbeauftragten weitere Pflichten übertragen werden. Dadurch kann die Koordination und Durchsetzung der notwendigen Datenschutzmaßnahmen im Unternehmen sichergestellt werden. Der Datenschutzbeauftragte kann leichter Fristen und Verpflichtungen, die sich aus der Datenschutz-Grundverordnung ergeben, wie die Pflicht zur Führung eines Verzeichnis von Verarbeitungstätigkeiten (Art 30 DSGVO), die Maßnahmen zur Datensicherheit (Art 32 DSGVO), die Einhaltung der Informationspflichten (Art 12 ff DSGVO) oder den zeitgerechten Abschluss von Dienstleistervereinbarungen (Art 29 DSGVO) 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 Punkte professionell beseitigt werden kann.

Erfahrung zählt - ganz besonders beim Datenschutz
Die ARGE DATEN organisiert seit 2006 mit großem Erfolg die Ausbildungsreihe „betrieblicher Datenschutzbeauftragter“. Mehr als 600 Personen haben den gesamten Lehrgang erfolgreich abgeschlossen, mehr als 3000 Personen haben einen oder mehrere Teile des Lehrgangs besucht. Vortragende des Lehrgangs sind namhafte Experten aus dem Universitätsbereich und der Wirtschaft. Wir können auf diese Weise fundiertes Fachwissen und klaren Praxisbezug garantieren. Laufend werden neue Entscheidungen und Entwicklungen in die Ausbildungsreihe integriert.

WARUM DAUERT DER LEHRGANG FÜNF TAGE?

Das Internet ist voll mit Instant-Lehrgängen von acht Stunden und weniger zum „perfekten“ Datenschutzbeauftragten. Datenschutz ist jedoch ein hochkomplexes Thema, dass sowohl umfassende technische, als auch rechtliche Anforderungen enthält.

Aus unserer Sicht sind fünf Tage, zwei mit Schwerpunkt Theorie, zwei mit Schwerpunkt Praxis und ein Intensiv-Workshop zur Umsetzung des erworbenen Wissens ein Minimum zum Einstieg in die Materie. Den „perfekten“ Datenschutzbeauftragten wird es wohl nie geben, unsere Teilnehmer erhalten jedoch Lösungsstrategien für höchst unterschiedliche Datenschutzfragen.

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.

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.

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.

ARGE DATEN - Zertifikat
Nach erfolgreicher Absolvierung des Abschlussmoduls wird dem „betrieblichen Datenschutzbeauftragten“ ein Zertifikat ausgestellt.

MODUL I: DATENSCHUTZ GRUNDLAGEN

Praxis, Entscheidungen, Perspektiven + inkl. Neuordnung des EU-Datenschutzes Das eintägige Seminar gibt eine kompakte Einführung in die wichtigsten Datenschutzgrundlagen und die rechtlich-organisatorischen Datensicherheitsanforderungen gem. der Datenschutz-Grundverordnung (DSGVO) und dem Datenschutz-Anpassungsgesetz 2018.
Diese Veranstaltung kann ohne besondere Voraussetzungen besucht werden.
Termine: 16. Oktober 2018, 9. April 2019

MODUL II: DATENVERWENDUNG IM UNTERNEHMEN

Vereinbarungen, Informationspflichten, Maßnahmen
Das eintägige Seminar konzentriert sich auf die besonderen betrieblichen Datenschutzanforderungen. Verpflichtungen zu Betriebsvereinbarungen mit den Mitarbeitern sind auf Informationspflichten nach dem E-Commerce-Gesetz und Mediengesetz gegenüber Kunden und Lieferanten abzustimmen. Datensicherheitsmaßnahmen haben den Datenschutz von Kunden und Mitarbeitern zu ergänzen.
Diese Veranstaltung kann ohne besondere Voraussetzungen besucht werden, empfohlen wird jedoch die Absolvierung der Veranstaltung "Modul I: Datenschutz Grundlagen" oder einer vergleichbaren Einführung in das Datenschutzrecht.
Termine: 17. Oktober 2018, 10. April 2019

MODUL III: DATENSCHUTZ UND IT-SICHERHEIT

Anforderungen, Konzepte, Umsetzung
Dieses Modul beschäftigt sich mit der Schnittstelle Datensicherheit und Datenschutz. Standards zur IT-Sicherheit, Fragen der korrekten Einschätzung von Sicherheitsanforderungen, Konzepte und Umsetzung von IT-Sicherheit und die Grundlagen einer optimalen Security Policy sind die Themen.
Diese Veranstaltung kann ohne besondere Voraussetzungen besucht werden, empfohlen wird jedoch die Absolvierung der Veranstaltung "Modul I: Datenschutz Grundlagen" oder einer vergleichbaren Einführung in das Datenschutzrecht.
Termine: 6. November 2018, 11. April 2019

MODUL IV: DATENSCHUTZ-GRUNDVERORDNUNG & PRAXIS

Erfahrungen, Unterschiede, Entwicklungen
Dieses Modul behandelt die europäische Datenschutzreform, Erfahrungen betrieblicher Datenschutzbeauftragter und rechtliche Fragen, die sich aus dem internationalen Datenverkehr ergeben. Schwerpunkt sind die Datenschutz-Grundverordnung und das Datenschutz-Anpassungsgesetz 2018.
Diese Veranstaltung kann ohne besondere Voraussetzungen besucht werden, empfohlen wird jedoch die Absolvierung der Veranstaltung "Modul I: Datenschutz Grundlagen" oder einer vergleichbaren Einführung in das Datenschutzrecht.
Termine: 18. Oktober 2018, 24. April 2019

MODUL V: WORKSHOP: DATENSCHUTZFRAGEN IM BETRIEB IDENTIFIZIEREN UND LÖSEN

Welche Datenverarbeitungen existieren im Unternehmen? Wie sind diese mit der DSGVO und dem Datenschutz-Anpassungsgesetz 2018 zu vereinbaren?
In dieser Veranstaltung mit Workshop-Charakter erarbeiten die Teilnehmer gemeinsam an Hand anonymisierter Fallbeispiele Lösungen zu den verschiedensten Datenschutzfragen und typischen Standardsituationen. Das Erlernte wird anhand eines Datenschutz-Quiz vertieft und mit der Durchführung einer Datenschutz-Folgenabschätzung in die Praxis umgesetzt. Weiters werden an Hand einer Checkliste optimale Datenschutzerklärungen (Privacy Statement) und verschiedene Zustimmungserklärungen analysiert.
Auf Grund des Workshop-Charakters findet diese Veranstaltung in Kleingruppen statt. Der Besuch der Module I bis IV ist Voraussetzung zur Teilnahme an dieser Veranstaltung.
Termine: 7. November 2018, 25. April 2019

TÄTIGKEITSBERICHT ARGE DATEN 2017/18

Beispiele aus der Beratungspraxis der ARGE DATEN
Dauerbrenner bei der Datenschutzberatung von Privatpersonen waren Smart Meter, ELGA und Bonitätsdaten. Schwerpunkt bei der Beratung der Datenverarbeiter war eine grundrechtskonforme Umsetzung der Datenschutz-Grundverordnung.

- **Energie:** Möglichkeiten Smart Meter Installationen abzulehnen
- **Gesundheit:** Opt-Out-Möglichkeiten bei ELGA
- **Bonität:** Löschung veralteter oder irreführender Bonitätsdaten
- **Statistik:** Verpflichtung zur Teilnahme an Mikrozensuserhebungen
- **Religion:** Löschungsansprüche nach Austritt
- **Arbeit:** Weitergabe von Gehaltsdaten an Dritte
- **DSGVO:** Informations- und Auskunftsrechte Betroffener
- **Gemeinden:** Veröffentlichungsrechte von Bürgerdaten
- **Arbeit:** Einsatz von Personalmanagementsystemen und Mitarbeiterbefragung
- **Gesundheit:** Verwendung von Patientendaten zu klinischen Prüfungen, Forschungs- und Unterrichtszwecken
- **Gesundheit:** Übermittlung von Gesundheitsdaten an US-Versicherung
- **Gesundheit:** Löschung von Gesundheitsdaten in einem Internet-Gesundheitsportal
- **Industrie:** Unterstützung im Aufbau von Datenschutzmanagement-Systemen
- **Verwaltung:** Untersützung bei Auskunftsbegehren
- **Gesundheit:** Zulässige Datenweitergabe bei Suchtberatung
- **Newsletter:** Gültigkeit von Einwilligungen beim elektronischen Newsletter-Bezug
- **Privatleben:** Zulässigkeit privater Videoüberwachung

Stellungnahmen
Im Zusammenhang mit dem Datenschutzanpassungsgesetz wurde im Juni 2017 von der ARGE DATEN eine umfangreiche und kritische Stellungnahme abgegeben.

Öffentlichkeitsarbeit, Informationsdienst
Im Rahmen unseres Mediendienstes und der Öffentlichkeitsarbeit erreichten wir regelmäßig zirka 5.000 datenschutzinteressierte Personen und konnten zahlreiche Medienanfragen zum Datenschutz beantworten.

Veranstaltungen, InHouse-Schulungen
2017 absolvierten 69 Teilnehmer den Lehrgang zum Datenschutzbeauftragten. Seit Beginn haben bisher mehr als 600 Personen den Lehrgang abgeschlossen.

21 Datenschutzveranstaltungen wurden 2017 von der ARGE DATEN organisiert, daran nahmen mehr als 800 Personen teil. Weiters wirkten Vertreter der ARGE DATEN an 20 weiteren Veranstaltungen mit und erreichten auf diese Weise rund 1000 Personen. In 9 Inhouse-Seminaren wurden etwa 200 Mitarbeiter in Datenschutzfragen geschult.

AUSKUNFTSRECHT NACH DER DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

DSGVO Art 4, 11-12, 15, 20, 26, 82-83; DSG § 24
Gemäß DSGVO haben Betroffene Auskunftsanspruch über die personenbezogenen Daten - auch wenn keine Berufung auf Datenschutzbestimmung erfolgt liegt Auskunftsanspruch vor - Auskunft ist unverzüglich zu erteilen, in jedem Fall innerhalb eines Monats - Auskunft ist in elektronischer Form zu geben - es sind auch pseudonymisierte Informationen zu beauskunften, sofern der Betroffene ausreichend mitwirkt - Branchen oder einzelne Organisationen könnten im Rahmen eines freiwilligen ‚Code of Conduct' kürzere Fristen festlegen - auch Erweiterungen des Auskunftsverfahrens im Rahmen eines ‚Code of Conduct' denkbar - bei fehlerhaften Auskünften drohen empfindliche Strafen und Schadenersatzforderungen

Das Auskunftsrecht ist als Betroffenenrecht im Datenschutzbereich von zentraler Bedeutung. Nur wenn Betroffene die Möglichkeit haben, sich einen Überblick über die sie betreffenden Datenströme zu verschaffen, können sie das grundlegende Recht auf informationelle Selbstbestimmung wahrnehmen. Möglichst vollständige Informationen über die von einem Verantwortlichen tatsächlich verarbeiteten Daten, deren Herkunft und die Empfänger von Übermittlungen bilden die unverzichtbare Basis für die Wahrnehmung aller weiteren Rechte wie zB Löschung oder Berichtigung von Daten, Einschränkung der Verarbeitung, Widerspruchsrecht usw.

Das Auskunftsrecht nach der Datenschutzgrundverordnung (DSGVO) kann als erster Schritt zu einem umfassenden Informationsfreiheitsrecht angesehen werden.

WO IST DAS AUSKUNFTSRECHT GEREGELT?

Das Auskunftsrecht ist auf mehreren Ebenen der Rechtsordnung geregelt und insofern mehrfach abgesichert. Auf europäischer Ebene findet sich die entsprechende Regelung in Art 15 der EU-Datenschutzgrundverordnung (Verordnung (EU) 2016/679 - DSGVO). Diese Verordnung kann Einzelnen unmittelbare Rechte einräumen und Pflichten auferlegen. Somit ist sie ohne Umsetzungsakt Bestandteil der österreichischen Rechtsordnung.

Die Bestimmungen der EU-Datenschutzgrundverordnung und des österreichischen Datenschutzgesetzes geben den allgemeinen Rahmen für das Auskunftsrecht vor. In Spezialgesetzen können besondere Vorschriften für die Erteilung von Auskünften vorgesehen werden. Ein Beispiel für eine solche Regelung ist der § 8 Abs 4 BilDokG, der die Vorgangsweise für die Auskunftserteilung aus der Bildungsevidenz regelt. Auch bei solchen speziellen Regelungen ist allerdings der vom Grundrecht vorgegebene Rahmen einzuhalten.

WEM STEHT DAS RECHT AUF AUSKUNFT ZU?

Nach der EU-Grundverordnungsbestimmung des Art 15 DSGVO hat der Betroffene das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, wozu sie verarbeitet werden, das Bestehen eines Berichtigungs-, Löschungs-, Einschränkungs- oder Widerspruchsrechts, das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde und voraussichtliche Speicherdauer der Daten, insbesondere auch, an wen sie übermittelt werden. Eine Auskunft kann natürlich nur erteilt werden, wenn tatsächlich Daten des Betroffenen gemäß Art 15 Abs 1 DSGVO verarbeitet werden. Andernfalls ist der Anfragende darüber zu informieren, dass keine Daten vorliegen.

WER IST ZUR AUSKUNFT VERPFLICHTET?

Der Adressat eines Auskunftsbegehrens ist gemäß Art 4 Z 4 DSGVO grundsätzlich der Verantwortlicher also jene natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über die Verwendung von personenbezogenen Daten entscheidet. Der Verantwortliche hat auch gemäß Art 12 Abs 1 DSGVO die Pflicht entsprechende technische und organisatorische Vorkehrungen zu treffen, die es ihm ermöglichen, seinen Pflichten gegenüber dem Betroffenen nachzukommen.

Gemäß Art 26 DSGVO sind Verantwortliche, die gemeinsam eine Datenverarbeitung durchführen, aufgefordert, mittels einer Zuständigkeitsvereinbarung festzustellen, wer über die Wahrnehmung des Auskunftsbegehrens nachkommt.

Aufgrund spezieller gesetzlicher Regelungen können auch andere Stellen für die Erteilung einer Auskunft zuständig sein (vgl. zB § 8 Abs 4 BilDokG).

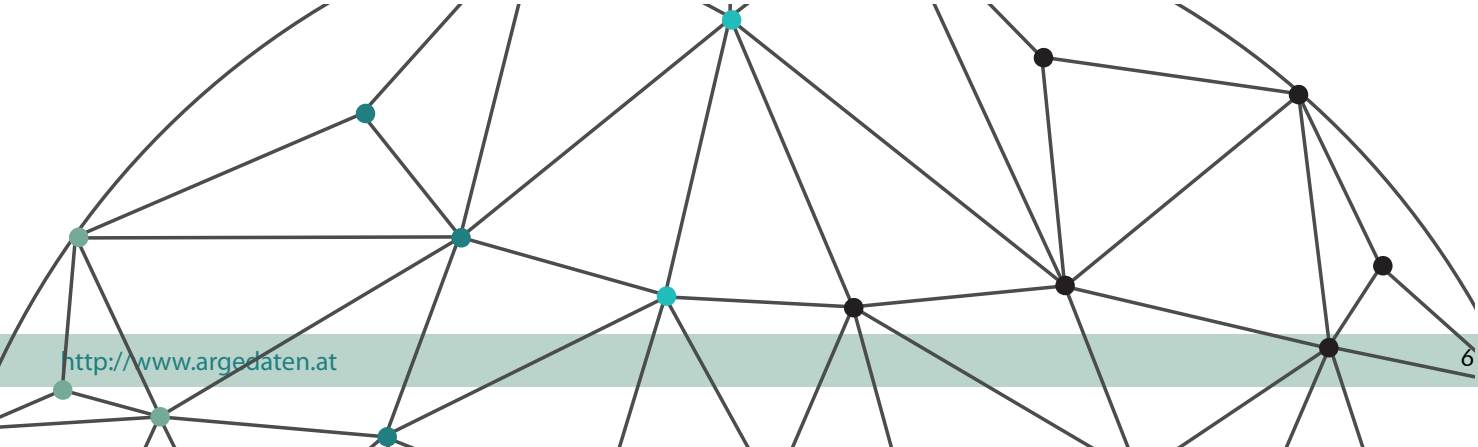
WELCHE DATEN SIND ZU BEAUSKUNFTEN?

Grundsätzlich sind alle Daten, die sich einer Person zuordnen lassen zu beauskunften. Dies betrifft sowohl Daten, die der Verantwortliche identifizierend einer Person zugeordnet hat (Kundendaten, Mitarbeiterdaten, Patientendaten, ...), als auch Daten, die er zwar einer Person nicht identifizierend zugeordnet hat, jedoch mit Hilfe des Antragstellers dem Betroffenen zuordnen kann. Das sind sogenannte pseudonymisierte Daten.

IN WELCHER FORM SIND DIE DATEN ZU BEAUSKUNFTEN?

Der Verantwortliche hat zu gewährleisten, dass eine Auskunft gemäß Art 12 DSGVO in transparenter und verständlicher Form erfolgt. Die Auskunftserteilung kann schriftlich oder elektronisch erfolgen. Weiters ist eine mündliche Beauskunftung zulässig, wenn die betroffene Person dies verlangt und die Identität des Betroffenen nachgewiesen wurde

Die DSGVO sieht grundsätzlich keine zwingende Formvorschrift hinsichtlich des Auskunftsansuchens vor. Bei berechtigter Zweifel über die Identität der betroffenen Person kann der Verantwortliche gemäß Art 12 Abs 6 DSGVO weitere Informationen verlangen. Der Betroffene der ein Auskunftsbegehren an einen Verantwortlichen richtet soll seine Identität nachweisen. Dies



soll verhindern, dass über den Weg eines Auskunftsbegehrens personenbezogene Daten in die Hände Unbefugter gelangen können. Die Kopie eines amtlichen Ausweises mit Unterschrift, ein Meldezettel usw. sind als Beispiele für die Anerkennung als Identitätsnachweis denkbar. Aus Beweisgründen sollten Auskunftsbegehren immer schriftlich gestellt werden. Für eine eventuell notwendige Beschwerde sollte der Versand möglichst vollständig dokumentiert werden (zB Einschreiben mit Rückschein, Faxsendebestätigung)

Nicht zulässig sind zusätzliche Voraussetzungen für die Erteilung einer Auskunft, die vom Verantwortlichen aufgestellt werden und die Auskunft für den Betroffenen erschweren sollen.

Die Auskunft selbst kann, sofern der Betroffene es nicht ausdrücklich anders wünscht, in elektronischer Form erfolgen. Dabei ist ein „gängiges Format" zu verwenden. Die DSGVO definiert nicht was ein „gängiges Format" ist. Gemeint ist offensichtlich, dass es kein Format sein darf, bei dem eine kostenpflichtige Zusatzsoftware erforderlich wäre, um die Auskunft lesen zu können. Damit soll vermieden werden, dass die grundsätzliche Kostenfreiheit (siehe unten) durch kostenpflichtige Leseprogramme unterlaufen wird. Eine Auskunft als pdf wird etwa diesen Ansprüchen entsprechen (zumindest solange ein pdf-Reader kostenlos bereitgestellt wird).

Zusätzlich besteht Anspruch auf Herausgabe jener Daten in strukturierter Form, die der Betroffene selbst bereitgestellt hat. Dies sind beispielsweise bei einem eMail-Betreiber die in der Mailbox eingetragenen eMail-Adressen, bei einem Telekom-Anbeiter die gespeicherten Telefon-Kontaktdaten, bei einem Facebook-Account, die hochgeladenen Bilder und Kommentare.

Diese Daten MÜSSEN so bereitgestellt werden, dass sie von einem anderen Unternehmen automatisiert übernommen werden können. Dieses Recht entspricht in etwa dem derzeit - auf freiwilliger Basis - angebotenen Service mancher Banken, bei Kontowechsel von Bank A nach Bank B, alle gespeicherten Daueraufträge usw. zu übernehmen.

Mit der DSGVO wird aus diesem Service ein gesetzlicher Anspruch!

KOSTEN

Grundsätzlich erfolgt die Auskunftserteilung an die betroffene Person kostenlos. Für den Fall, dass der Betroffene über die kostenlos zur Verfügung gestellte Kopie hinaus weitere Kopien anordnet, kann der Verantwortliche gemäß Art 15 Abs 3 DSGVO ein angemessenes Entgelt verlangen. Weiters bei offenkundig unbegründeten oder exzessiven Anträgen eines Betroffenen kann der Verantwortliche entweder ein angemessenes Entgelt verlangen oder er weigert den Antrag in Bearbeitung zu nehmen.

Die unentgeltliche Bearbeitung von Auskunftsbegehren ist erfahrungsgemäß nicht selbstverständlich. In einem Fall wurden ein Betroffener von einem großen Mobilfunkbetreiber an eine Mehrwertnummer verwiesen, unter der er angeblich Auskunft erhalten würde. In einer Stellungnahme gab das Unternehmen später an, dass es sich dabei um ein Versehen gehandelt habe und die Auskunft kostenlos wäre. Eine derartige Vorgangsweise wäre DSGVO-widrig.

FRIST

Eine Auskunft ist unverzüglich, in jedem Fall innerhalb von einem Monat nach Einlangen beim Verantwortlichen zu erteilen bzw. es ist innerhalb dieser Frist zu begründen, warum keine Auskunft erteilt wird. Wenn innerhalb dieser Frist (evtl. inkl. Postlauf) keinerlei Reaktion auf das Auskunftsbegehren erfolgt, liegt jedenfalls eine Verletzung des Auskunftsrechts vor. Bei komplexeren Anspruchsbegehren kann die Frist um zweite weitere Monate verlängert werden. Der Betroffene muss über die Fristverlängerung verständigt werden und zwar in Anführung der Gründe.

AUSNAHMEN VOM AUSKUNFTSRECHT

Die Beauskunftung kann in sechs Fällen, die im § 43 Abs 4 Datenschutzgesetz (DSG) angeführt sind, soweit und solange aufgeschoben, eingeschränkt oder unterlassen werden:

1. zur Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden, insbesondere durch die Behinderung behördlicher oder gerichtlicher Untersuchungen, Ermittlungen oder Verfahren
2. zum Schutz der öffentlichen Sicherheit
3. zum Schutz der nationalen Sicherheit
4. zum Schutz der verfassungsmäßigen Einrichtung der Republik Österreich
5. zum Schutz der militärischen Eigensicherung oder
6. zum Schutz der Rechte und Freiheiten anderer

MÜSSEN DIE EMPFÄNGER VON ÜBERMITTLUNGEN BEAUSKUNFTET WERDEN?

Die Auskunft eines Verantwortlichen muss nach der DSGVO auch allfällige Empfänger oder Empfängerkreise umfassen. Die Bekanntgabe der Übermittlungsempfänger ist eine Grundlage des Rechts auf informationelle Selbstbestimmung, weil nur so Datenströme, die sich auf eine Person beziehen, nachverfolgt und von dieser Person kontrolliert werden können.

Sind konkrete Übermittlungen erfolgt, sind die Empfänger bekannt zu geben. Ausnahmen davon wären nur in ganz speziellen Fällen (zB Schikaneverbot) zulässig.

Bei Bonitätsauskünften muss beauskunftet werden, woher die Daten stammen, weil ein besonderes Interesse des Betroffenen besteht seine Betroffenenrechte sowohl bei der Quelle als auch bei den Empfängern der Daten geltend zu machen. Eine Verletzung der Geheimhaltungsinteressen der Übermittlungsempfänger ist grundsätzlich nicht anzunehmen.

MUSS DIE HERKUNFT DER DATEN BEKANNT GEGEBEN WERDEN?

Nach dem Wortlaut der DSGVO Art 15 ist nur über die verfügbaren Daten Auskunft zu erteilen. Eine andere Regelung ist offensichtlich auch gar nicht möglich.

In der DSGVO sieht der Erwägungsgrund 66 vor, dass vom Verantwortliche angemessene Maßnahmen zum Schutz der Rechte der Betroffenen vorzusehen sind. Dies ist wohl so zu verstehen, dass zu mindestens grundsätzlich die Herkunft von Daten in einer Weise zu protokollieren ist, die auch eine Auskunftserteilung an die Betroffenen ermöglicht.

Bei Bonitätsauskünften muss beauskunftet werden, woher die Daten stammen, weil ein besonderes Interesse des Betroffenen besteht seine Betroffenenrechte sowohl bei der Quelle als auch bei den Empfängern der Daten geltend zu machen.

DURCHSETZUNG DES AUSKUNFTSRECHTS

Zur Durchsetzung des Rechts auf Auskunft - ob im privaten oder öffentlichen Bereich - ist gemäß § 24 DSG eine Beschwerde bei der Datenschutzbehörde vorgesehen.

Der Vorteil einer Beschwerde bei der Datenschutzbehörde ist, dass diese kostenfrei und ohne die Vertretung durch einen

Anwalt eingebracht werden kann. Die Datenschutzbehörde führt dann ein Ermittlungsverfahren durch und erlässt schlussendlich einen Bescheid, der gegebenenfalls exekutiert werden kann.

Das Datenschutzgesetz gewährleistet, gegen Bescheide der Datenschutzbehörde und für den Fall, dass diese ihren Ermittlungspflichten nicht zeitgerecht nachkommt, eine Beschwerde an das Bundesverwaltungsgericht zu erheben.

AUSKUNFT VON VERANTWORTLICHEN IM AUSLAND

Durch die EU-Datenschutzverordnung wurde gezielt eine EU-weite Harmonisierung der Datenschutzgesetzgebung zu erreichen. Es ist demnach davon auszugehen, dass in allen Mitgliedsstaaten der Europäischen Union ein durchsetzbares Auskunftsrecht besteht. Die Mitgliedstaaten sind begrüßt nationale Regelungen von anderen Details gemäß der DSGVO zu bestimmen.

Besonders im Hinblick auf die Möglichkeiten zur Rechtsdurchsetzung ist gemäß der DSGVO in den verschiedenen Ländern von ähnlichen Voraussetzungen auszugehen.

In Ländern, die nicht Mitglied der EU oder des EWR sind, wird die Durchsetzung von Auskunftsbegehren vielfach nur schwer möglich sein. Allerdings ist in jenen Ländern, denen von der EU-Kommission die Gleichwertigkeit mit den europäischen Regelungen bescheinigt wurde, davon auszugehen, dass auch ein Auskunftsanspruch besteht.

BEI AUSKUNFT FREIWILLIG KÜRZERE FRISTEN EINHALTEN

Alle bisher besprochenen Auskunftsregeln ergeben sich aus den gesetzlichen Bestimmungen der EU-Datenschutzgrundverordnung und des österreichischen Datenschutzgesetzes. Diese Auskunftsrechte können auch nicht privatrechtlich, etwa durch entsprechend formulierte AGBs ausgeschlossen werden. Derartige Formulierungen, wie „beide Vertragspartner verzichten auf das Auskunftsrecht gemäß EU-Datenschutzgrundverordnung und Datenschutzgesetz“ sind rechtsunwirksam.

Es besteht jedoch für Verantwortlichen die Möglichkeit die Auskunftsfristen zugunsten des Betroffenen zu verkürzen bzw. den Auskunftsumfang freiwillig zu erweitern. Eine wichtige Erweiterung wäre etwa, bekannt zu geben welche Auswertungen mit den persönlichen Daten gemacht werden.

Derartige Erweiterungen könnten branchenweit durch gemeinsame Datenschutzstandards („Code of Conduct“) formuliert werden, oder unternehmensspezifisch durch sogenannte Privacy-Statement. Leider gibt es dazu kaum lobenswerte Beispiele oder Initiativen.

STRAFEN UND SCHADENERSATZ

Fehlerhafte Auskünfte können mit bis zu 20 Millionen Euro Strafe oder 4 % des weltwiten Jahresumsatzes bestraft werden, je nach dem was höher ist. Nun ist nicht zu erwarten, dass die Aufsichtsbehörde diese Strafe bei einem kleinen Versehen verhängen wird, wohl aber wenn das Auskunftsbegehren systematisch gegenüber vielen Betroffenen ignoriert wird. Verantwortliche großer Datenverarbeitungen sollten daher zeitgerecht Prozesse für eine exakte Auskunftserteilung vorbereiten.

Zusätzlich kann ein Betroffener Schadenersatz bei fehlerhafter Auskunft verlangen. Dies ist gegenüber dem DSG 2000 eine völlig neue Rechtsmöglichkeit. Ein Betroffener kann dabei recht erfolgreich argumentieren, dass eine Verzögerung in der Auskunft ihn einerseits in der Wahrnehmung weiterer Betroffenenrechte behindert, andererseits er dadurch in seinem Recht auf informationelle Selbstbestimmung beschränkt wurde und damit Grund- und Freiheitsrechte beschränkt wurden.

Die DSGVO sieht zwar keine Mindesthöhe im Schadenersatz vor, bisherige Gerichtsentscheidungen nach den alten DSG 2000 -

Bestimmungen haben jedoch festgehalten, dass 750,- Euro auch bei minimalen Vergehen gerechtfertigt sind. Betroffene werden daher eine Schadenshöhe von 1.000,- Euro auch dann beanspruchen können, wenn der Eingriff in ihre Freiheitsrechte nur geringfügig ist. Ein Betrag, der im Einzelfall wohl verkraftbar ist, sind jedoch mehrere 1000 Personen betroffen, kann dieser Anspruch rasch teurer werden, als die eigentlichen Strafdrohungen.

INFORMATIONSPFLICHTEN DER DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

DSGVO Art 13-14, 82-83
Informationen die dem Betroffenen mitgeteilt werden müssen - leichte Zugänglichkeit entscheidet - Profiling und automatisierte Entscheidungsfindung - Geldstrafe und Schadenersatz drohen

Eine transparente Datenverarbeitung ist ein wesentliches Anliegen der DSGVO. Um dies zu verwirklichen, sind Verantwortliche verpflichtet die Betroffenen aktiv von sich aus über ihre Datenverarbeitungen zu informieren.

Die DSGVO unterscheidet bei den Informationspflichten zwischen der Datenerhebung bei der betroffenen Person (Bsp: Befragung mittels Formular) und der Datenerhebung aus anderen Quellen (Bsp: Ermittlung von Daten durch Kreditschutzverband).

DATENERHEBUNG DIREKT BEI DER BETROFFENEN PERSON

Werden die Daten beim Betroffenen erhoben, müssen Basisdaten zur Organisation und Detailinformationen zu den Verarbeitungen bekannt gegeben werden.

BASISDATEN:

- Kontaktdaten des Verantwortlichen
- Verarbeitungszwecke und Rechtsgrundlage der Verarbeitung
- Kontaktdaten des Datenschutzbeauftragten (wenn eine Organisation einen Datenschutzbeauftragten hat)
- im Falle einer Datenverarbeitung aufgrund berechtigter Interessen des Verantwortlichen bzw. eines Dritten
- bei Datenübermittlung: Empfänger oder Kategorien von Empfängern
- Angabe ob die Daten an ein Drittland oder eine internationale Organisation übermittelt werden

VERARBEITUNGSDATEN:

- Dauer oder Kriterien der Dauer, für die die personenbezogenen Daten gespeichert werden
- Informationen zu den Betroffenenrechten: Auskunftsrecht, Recht auf Berichtigung oder Löschung, Recht auf Einschränkung der Verarbeitung, Widerspruchsrecht gegen die Verarbeitung, das Recht auf Datenübertragbarkeit
- Informationen zum Widerrufsrecht (bei Verarbeitung auf Grund freiwilliger Zustimmung)
- Informationen zum Beschwerderecht bei einer Aufsichtsbehörde
- Information, ob die ermittelten Daten gesetzlich vorgeschrieben, vertraglich verpflichtend oder für einen Vertragsabschluss erforderlich sind
- Information, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen und welche möglichen Folgen die Nichtbereitstellung hätte
- Information, ob automatisierte Entscheidungsfindung, Scoring, Profiling oder Vergleichbares stattfinden

AUSNAHMEN VON DER INFORMATIONSPFLICHT

Die Informationspflicht des Verantwortlichen entfällt, wenn die betroffene Person bereits die Informationen kennt. Erfolgte die Ermittlung vor in Kraft treten der DSGVO, dann ist keine nachträgliche Information erforderlich. Werden jedoch Daten nacherhoben, korrigiert oder ergänzt, dann ist der volle Informationsumfang zu beachten.

Spätestens jedoch bei einem Auskunftsbegehren müssen die angegebenen Informationen auch jenen Betroffenen bekannt gegeben werden, bei denen die Erhebung vor In Kraft treten erfolgte.

FORM UND KOSTEN DER INFORMATION

Die Ankündigung der Informationen soll in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache (auch in elektronischer Form) erfolgen. Die Bereitstellung der Informationen erfolgt grundsätzlich kostenlos. Ein Anspruch auf Kostenersatz besteht nur bei offenkundig unbegründeten oder exzessiven Anträgen.

Die ARGE DATEN empfiehlt die Informationen gemäß DSGVO auf der Webseite des Verarbeiters zu veröffentlichen. Im Falle eines persönlichen Kunden- oder Klienten-Verkehrs (etwa bei einem Arzt) sollten diese Informationen in geeigneter Form ausgehängt oder eine Broschüre (ein Infoblatt) bereitgestellt werden. Bei Videoüberwachungen sollte ein Schild am Eingang deutlich darauf hinweisen und die Identität des Verantwortlichen offenlegen.

INFORMATION ÜBER DIE WEITERVERWENDUNG FÜR ANDERE ZWECKE

Wenn der Verantwortliche beabsichtigt die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten, außer den dafür vorgesehenen, so muss die betroffene Person auch darüber informiert werden.

DATENERHEBUNG OHNE DIREKTEN KONTAKT ZUM BETROFFENEN

Bei diesen Datenerhebungen stammen die Daten aus einer anderen Quelle als dem Betroffenen stammen. Hier ist die allgemeine Informationspflicht einzuhalten und zu beauskunften, aus welcher Quelle die Daten stammen.

ZEITPUNKT DER INFORMATION

Werden die Daten nicht beim Betroffenen erhoben, muss der Verantwortliche den Betroffenen grundsätzlich innerhalb einer angemessenen Frist informieren, spätestens jedoch nach einen Monat. Sollten die Daten zur Kommunikation mit dem Betroffenen verwendet werden, dann sind die erforderlichen Informationen spätestens zum Zeitpunkt der ersten Mitteilung an den Betroffenen zu geben. Wenn die Offenlegung an einen anderen Empfänger beabsichtigt ist, hat die Information zum Zeitpunkt der ersten Offenlegung zu erfolgen.

ZUSÄTZLICHE EINSCHRÄNKUNGEN DER INFORMATIONSPFLICHT WENN ERHEBUNG NICHT BEIM BETROFFENEN LIEGT

Die Informationspflicht des Verantwortlichen entfällt, wenn Rechtsvorschriften die Datenerhebung ausdrücklich erlauben oder die Informationen rechtlicher Geheimhaltungspflichten unterliegen. Letztlich besteht auch dann keine Informationspflicht, wenn die Erteilung der Information für den Verantwortlichen unmöglich ist oder zumindest mit einem unverhältnismäßigen Aufwand verbunden ist.

PROFILING UND AUTOMATISIERTE ENTSCHEIDUNGSFINDUNG

Profiling und automatisierte Entscheidungsfindung sind beispielsweise im Bank- und Finanzwesen, im Steuerbereich und in der Gesundheitsversorgung gängige Praxis.

Profiling ist die Bezeichnung für das Erstellen, Aktualisieren und Verwenden von Profilen aus gesammelten Daten (Alter, Geschlecht, Einkommen, …). Diese Profile werden zu Marktforschungszwecken verwendet.
Beispielsweise nutzt ein Betroffener für ein Darlehen eine Online-Bank. Er wird aufgefordert seine personenbezogenen Daten einzugeben. Folglich teilt der Algorithmus der Bank mit, ob die Bank das Darlehen gewährt und wie hoch der vorgeschlagene Zinssatz ist.

Eine automatisierte Entscheidungsfindung liegt vor, wenn Entscheidungen über einen Betroffenen auf technischem Wege und ohne menschliches Eingreifen getroffen werden. Gemäß DSGVO sind Verantwortliche auch verpflichtet über das Bestehen eines Profiling und einer automatischen Entscheidungsfindung zu informieren. Angaben über die involvierte Logik, die Tragweite und die angestrebten Auswirkungen der automatischen Entscheidungsfindung bzw. des Profiling sollten im Informationsblatt enthalten sein.

GELDSTRAFE UND SCHADENERSATZ DROHEN

Bei Verstößen gegen den Schutz personenbezogener Daten oder Nichtgewährleistung einer fairen und transparenten Datenverarbeitung drohen hohe Geldstrafen von bis zu 20 Mio. Euro und bei Unternehmen von bis zu 4% des letzten weltweiten Jahresumsatzes (Art 83 Abs 5 DSGVO). Die Datenschutzbehörde entscheidet über die Verhängung von Geldstrafen. Des Weiteren können Betroffene Schadenersatz geltend machen (Art 82 DSGVO). Landesverwaltungsgerichte sind zuständig für Schadenersatzklagen.

MELDEPFLICHTEN DER VERANTWORTLICHEN BEI DATENSCHUTZ-VERLETZUNGEN

DSGVO Art. 33, 34, 82, 83
Meldepflicht gegenüber Datenschutzbehörde und gegenüber Betroffenen - Einschränkung der Meldepflicht gegenüber Betroffenen nur bei Wahrscheinlichkeit eines hohen Risikos - Meldepflicht gilt auch bei Verlust von Geräten wie Smartphone, Notebook oder USB-Stick, wenn sie personenbezogene Daten enthalten

SCHON BISHER VERSTÄNDIGUNGSPFLICHT DER BETROFFENEN

Schon im DSG 2000 gibt es gemäß § 24 Abs. 2a bei Datenschutzverletzungen eine Meldepflicht gegenüber dem Betroffenen. Dies jedoch nur im Zusammenhang mit einem hohen Risiko für den Betroffenen, wenn die Datenschutzverletzung schwerwiegend war, zahlreiche Personen betraf und wenn die Verständigung nicht allzu aufwändig ist. Eine Art Verständigungspflicht „light".

In den letzten Jahren kam es zu zahlreichen derartigen Verständigungen, unter anderem im Zusammenhang mit der GIS, einiger österreichischer Energieversorger und Verkehrsunternehmen.

Ignoriert wurde die Meldepflicht im Zusammenhang mit dem größten Datenschutzskandal der Republik, der rechtswidrigen Weitergabe von mehreren Millionen Exekutionsdatensätzen an Wirtschaftsauskunftsdienste. Hier stand das Justizministerium auf den Standpunkt, die öffentliche Berichterstattung wäre ausreichend.

MASSIVE AUSWEITUNG DER MELDEPFLICHT

Mit der neuen Datenschutzgrundverordnung (DSGVO) wird die Meldepflicht drastisch ausgeweitet. Zum einen besteht eine Meldepflicht bei jeder Datenschutzverletzung an die Datenschutzbehörde. Diese kann nur dann entfallen, wenn kein Risiko für die Betroffenen besteht. Schon im Fall eines geringen Risikos besteht die Meldepflicht. Kein Risiko wird dann bestehen, wenn verlorene Daten so stark verschlüsselt sind, dass sie mit den heute bekannten Techniken nicht entschlüsselt werden können. Dies wird bei Daten auf zertifizierten Smartcards oder HSM-Systemen der Fall sein (HSM = Hardware Security Modules). Auch eine Kombina-

tion von zertifizierten biometrischen Verfahren und Zwei-Faktor-Authentisierung kann als ausreichende Sicherheitsmaßnahme angesehen werden.

Verlorene Geräte mit personenbezogenen Daten, die nur über einen Zugriffsschutz mittels Passwort verfügen, werden nicht ausreichend abgesichert sein. Auch die Schutzmechanismen bekannter Betriebssysteme sind leicht zu umgehen und daher bestenfalls unter die Rubrik Sicherheitsfolklore einzuordnen.

Gegenüber Betroffenen besteht die beschränkte Verständigungspflicht bei einem möglichen hohen Risiko „für die Rechte und Freiheiten des Betroffenen". Klargestellt wurde jedoch, dass Betroffene persönlich zu informieren sind. Nur wo dies nicht möglich ist, können vergleichbar effektive Alternativen genutzt werden.

Alternativ kann die Datenschutzbehörde Betroffene informieren, etwa wenn sich ein Verantwortlicher weigert seinen Meldepflichten nachzukommen.

UMFASSENDE MELDEPFLICHT GEGENÜBER DATENSCHUTZBEHÖRDE

Der Datenschutzbehörde sind folgende Informationen zu geben:

- Beschreibung der Art der Datenschutzverletzung
- Name und Kontaktstelle die über den Vorfall Auskunft geben kann
- (Datenschutzbeauftragter oder sonstige Anlaufstelle)
- Beschreibung der wahrscheinlichen Folgen für Betroffene
- Beschreibung der ergriffenen Maßnahmen
- Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Daten-Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze

Die Meldung hat binnen 72 Stunden zu erfolgen, kann aber - abhängig vom Sachverhalt - auch schrittweise erfolgen. Nur wenn die Ermittlung der Datenschutzverletzung aufwändig ist oder sonstige Unklarheiten bestehen, kann die Meldung später erfolgen. Die Verspätung ist jedoch zu begründen.

Die Meldepflicht besteht auch dann, wenn dem Verantwortlichen kein Verschulden an der Datenschutzverletzung trifft, etwa weil sich eine von ihm verwendete Software oder Hardware nachträglich als fehlerhaft oder unzuverlässig entpuppt hat.

EINGESCHRÄNKTE MELDEPFLICHT GEGENÜBER BETROFFENEN

Die Meldepflicht gegenüber dem Betroffenen ist grundsätzlich ident. Nicht meldepflichtig an den Betroffenen sind jedoch Angaben über die Zahl der betroffenen Personen, der Kategorien der Personen oder die Zahl der betroffenen Datensätze.

Die Meldepflicht kann entfallen, wenn kein hohes Risiko für den Betroffenen besteht oder nachträgliche Maßnahmen das Risiko reduzieren. Dies wird dann der Fall sein, wenn Zugangskennungen nach Korrumpierung unverzüglich gesperrt werden.

Die Meldung kann auch entfallen, wenn technische und/oder organisatorische Sicherheitsmaßnahmen den Zugriff auf die betroffenen Daten verhindern. Dies wird bei geeigneten Verschlüsselungen der Fall sein.

INTERNES DATENSCHUTZMANAGEMENT ERFORDERLICH

Das eigentliche Problem der umfassenden Meldepflichten sind weniger die einzelnen Datenschutzverletzungen, als die Verpflichtung rasch zu reagieren.

Schon der Verlust eines Mobiltelefons kann Meldepflicht auslösen. Bisher war der Verlust eines Firmenhandys eine interne Angelegenheit zwischen Mitarbeiter, seinem Vorgesetzten und der Einkaufsabteilung. Schlimmstenfalls wurde die Kostenstelle der Mitarbeiterabteilung mit einigen hundert Euro Aufwand belastet und das Handy beim Mobilfunkbetreiber gesperrt bzw. abgemeldet.

Jetzt muss geprüft werden, in welchem Umfang personenbezogene Daten betroffen sind und rasch jedenfalls an die Datenschutzbehörde gemeldet werden. Das Informationsmanagement bei Verlust von Datenträgern MUSS im Unternehmen innerbetrieblich zentral gesteuert werden. In großen Unternehmen mit vielen Standorten eine echte Herausforderung, auf die man sich schon jetzt vorbereiten sollte. Bei der ersten Datenschutzverletzung ist es zu spät.

ZAHLREICHE DATENSCHUTZSCHWACHSTELLEN MÖGLICH

Neben verlorenen Datenträgern (Smartphone, USB-Stick, Notebook, DVD, ausgedruckte Listen) gibt es zahllose weitere Bereiche, die zu Datenschutzverletzungen führen können.

Potentielle Schwachstellen (Auszug):

- fehlerhafte Eingabemasken, die zu falsch ermittelten Daten führen
- ungeeignete biometrische Identifikationssysteme, die den falschen Personen Zugriff oder Zugang gewähren
- Sicherheitslücken auf Grund
- fehlerhafter Hard- oder Software
- fehlerhafte Scoringmechanismen,
- die falsche Bewertungen durchführen
- fehlerhafte Lösch- und Backup-Prozesse, die keine Wiederherstellung notwendiger Daten erlauben
- unzureichende Sicherungsmechanismen, die Angriffe durch externe und interne Täter erlauben
- fehlerhaft adressierte eMails

Neben einem effizienten Meldeverfahren sind daher die Datenverarbeiter mehr als bisher gefordert Datenschutzschwachstellen zu identifizieren und versuchte Verletzungen zu erkennen.

In Hochsicherheitsbereichen, etwa im Gesundheitswesen, werden Verarbeiter ohne einem Dokumentenmanagementsystem, Verschlüsselung und elektronischer Signatur, qualifizierte Zeitstempelsysteme, Intrution-Detection-Systeme, redundante Verständigungssysteme und revisionssicherem Logging nicht auskommen.

Die DSGVO verlangt nichts davon ausdrücklich, um jedoch auditierbar zu bleiben oder auch eine Datenschutz-Zertifizierung zu bekommen, wird darum kein Weg herumführen.

HOHE SANKTIONSDROHUNG

Eine Missachtung der Meldepflichten ist mit Geldbußen bis 10 Millionen Euro oder 2 % des Jahresumsatzes zu ahnden, je nachdem was höher ist. Zusätzlich können Betroffene Schadenersatz verlangen. Dies gilt für erlittene materielle Schäden, etwa Zusatzkosten die durch Ausstellung neuer Dokumente oder Zahlungshilfsmittel (Kreditkarten) entstehen können.

Der Schadensersatzanspruch gilt jedoch auch für „immaterielle“ Schäden, also auch für die Verunsicherungen und Sorgen die eine derartige Datenschutzverletzung auslösen. Im Gegensatz zu früher ist dabei eine „bloßstellende Veröffentlichung“ persönlicher Daten nicht mehr Erfordernis für den Schadensersatzanspruch.

Es gibt keine Untergrenze in der Schadenshöhe aber auch keine Obergrenze. Ein minimaler Pauschalwert von 1.000,- Euro für die erlittenen „immateriellen“ Schäden je Person ist angesichts bisheriger OGH-Entscheidungen realistisch. Sind mehrere tausend Menschen davon betroffen, kann sich die Schadensersatzforderung rasch in Millionenhöhe bewegen.

LÖSCHUNGS- UND BERICHTIGUNGSPFLICHT - VERSTÄNDIGUNG DER EMPFÄNGER

DSGVO Art 5, 15-17, 19, 21; GewO § 151
Löschungsgründe - Ausnahmen von der Löschungspflicht - Löschen im Sinne der DSGVO - Verarbeitung von veralteten oder falschen Daten - Rechte der Betroffenen (Kunden) - Richtige Reaktion auf Löschungsbegehren - Sonderfall Marketing - Mitteilungs- und Informationspflicht des Verantwortlichen - Fristen - Beschwerde- und Schadenersatzrecht

Grundsätzlich sind unvollständige Daten zu ergänzen, veraltete Daten zu berichtigen und nicht mehr benötigte Daten oder unberechtigt verarbeitete Daten zu löschen.

Zunächst muss die betroffene Person natürlich Kenntnis von den über sie gespeicherten Daten haben. Hier hilft ihr das Auskunftsrecht aus Art. 15 der Datenschutz-Grundverordnung (DSGVO) weiter. Wird die Löschung abgelehnt, ist dies vom Verantwortlichen zu begründen. Auf die Möglichkeit zur Beschwerde bei einer Aufsichtsbehörde und auf einen gerichtlichen Rechtsbehelf ist hinzuweisen. Davon abgesehen sind in der Regel auch unvollständige Daten zu berichtigen und nicht mehr benötigte Daten oder unberechtigt ermittelte bzw. verwendete Daten zu löschen.

LÖSCHUNGSGRÜNDE

Art 17 DSGVO regelt das Löschungsrecht bei Vorliegen bestimmter Löschungsgründe.

Als Löschungsgründe kommen in Betracht:

- ein Wegfall des Verarbeitungszwecks
- ein Widerruf der Einwilligung des Betroffenen
- ein wirksamer Widerspruch gemäß Art 21 DSGVO
- eine Unrechtmäßigkeit der Datenverarbeitung,
- eine rechtliche Verpflichtung zur Löschung (Gesetz, Urteil, Bescheid)
- die personenbezogenen Daten eines Kindes wurden in Bezug auf angebotene Dienste der Informationsgesellschaft erhoben (beispielsweise Fehlen einer Einwilligung der Erziehungsberechtigten eines Kindes)

Demnach sind verordnungswidrig verarbeitete Daten zu löschen sobald die Unzulässigkeit bekannt wird oder ein Betroffener (Kunde) einen begründeten Antrag auf Löschung stellt. Unzulässig ist eine Datenverarbeitung grundsätzlich immer dann, wenn dieser kein rechtmäßiger Zweck mehr zugrunde liegt (Art 5 Abs lit b DSGVO).

Im Fall, dass ein und dieselben Daten für mehrere Zwecke verarbeitet werden, dürfen diese erst gelöscht werden, wenn sämtliche Verarbeitungszwecke wegfallen.

Damit sind die Aktualisierung bzw. das Löschen von Daten bei Wegfall des Verarbeitungszwecks durchzuführen. Dies kann durch den Betroffenen erfolgen, aber auch indem Post retourniert wird oder Dritte auf veraltete oder falsche Daten hinweisen. In diesem Fall sind falsche Daten richtigzustellen und nicht mehr benötigte Daten zu löschen.

Die Löschungspflicht des Verantwortlichen ist weiteres gegeben, wenn eine unrechtmäßige Datenverarbeitung erfolgte oder die Datenlöschung von rechtlicher Bedeutung ist. Beispielsweise kann eine gesetzliche Vorschrift oder ein Urteil oder ein Bescheid die Löschungspflicht anordnen. Der Verantwortliche muss Daten löschen, wenn der Betroffene der Verarbeitung widerspricht, sofern keine vorrangig berechtigten Gründe eine Verarbeitung existieren. Daten eines Kindes sind allenfalls bei Fehlen einer Einwilligung der Erziehungsberechtigten zu löschen.

AUSNAHMEN VON DER LÖSCHUNGSPFLICHT

Die DSGVO regelt auch Ausnahmefälle, die von der Löschungspflicht nicht umfasst sind. Das Löschungsbegehren wird dann keinen Erfolg haben, wenn die Verarbeitung erforderlich ist oder bei Ausübung des Rechts auf freie Meinungsäußerung der Information. Weiters besteht keine Löschungspflicht zur Erfüllung einer Rechtspflicht oder öffentlicher Aufgaben.

Der Verantwortliche ist nicht zur Löschung verpflichtet bei Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit oder bei öffentlichen Interesse liegenden Archivzwecken, Forschungszwecken und statistischen Zwecken.

VERARBEITUNG VON VERALTETEN ODER FALSCHEN DATEN

Dies hängt wesentlich vom Zweck der Datenverwendung ab. In einer bloß intern verwendeten Marketing- und Interessentendatei wird es nicht notwendig sein, ständig Anschrift, Telefonnummer, Fax, ... nach der Aktualität zu überprüfen. Bei der nächsten Verwendung oder Postaussendung wird man auf Grund der Retouren und missglückter Kontakte feststellen, welche Daten nicht mehr aktuell sind und diese korrigieren.

Schwierigkeiten entstehen dort,

a. wo Dritte, aus eigenem Antrieb Daten für eigene Zwecke sammeln oder
b. wo Daten an Dritte für Zwecke weitergegeben werden (nicht immer im Interesse des Betroffenen).

Ein typisches Beispiel zu Fall (a) sind die Unmengen von Verzeichnissen, Datenbanken und Linklisten, die im Internet als Telefonbücher, Mail-Verzeichnisse oder Branchenverzeichnisse existieren. Meist werden diese Daten einmal übernommen und nicht mehr weiter gepflegt. Alte Informationen können Benutzer in die Irre führen oder sind schlicht ärgerlich.

Manche dieser Online-Verzeichnisse halten Update-Funktionen bereit, mit denen Betroffene selbst Daten pflegen können, die meisten ermöglichen keinerlei Online-Änderungen. In der Regel wird das bloße Bereitstellen einer Updatefunktion nicht ausreichen, sondern der Anbieter muss eigene Maßnahmen zur Erfüllung der Aktualisierungspflicht treffen. Dies umso mehr, als viele Betroffene gar nicht wissen, dass sie in einem bestimmten Informationssystem enthalten sind.

Wesentlich schwerwiegender ist Fall (b), etwa im Zusammenhang

mit Wirtschaftsauskunftsdiensten und Gläubigerschutzverbänden. Falsche oder veraltete Daten können kreditschädigend sein oder den Zugang von Personen zum wirtschaftlichen Leben verteuern oder unmöglich machen. Vielfach melden Finanzdienstleister an den KSV 1870, dass sie ‚Kreditanträge abgelehnt' hätten oder ein Kunde in ‚Zahlungsverzug geraten sei', ohne die tatsächlichen Begleitumstände darzulegen bzw. festzuhalten, wie aktuell diese Information ist. Hier besteht von Seiten des Betroffenen ein Aktualisierungs- und Klarstellungsrecht, dass alle notwendigen Begleitumstände derartiger schwerwiegender Feststellungen darlegt.

Aber auch von Seiten des meldenden Geldinstituts und des KSV besteht eine aktive Aktualisierungspflicht. In regelmäßigen Abständen, per Bescheid der Datenschutzbehörde zumindest einmal jährlich, haben diese Stellen zu überprüfen, ob die gespeicherten, verwendeten und veröffentlichten Informationen noch vollständig und richtig sind. Kredite können ganz oder teilweise zurückgezahlt sein, ein Zahlungsverzug kann bereinigt sein, bei Zahlungsproblemen kann es zu einer einvernehmlichen Lösung zwischen Betroffenen und Bank gekommen sein.

Nach den bisherigen Erfahrungen stehen Verantwortliche im Bereich der Wirtschaftsauskunftsdienste meist auf dem Standpunkt, dass alles was sie tun ‚berechtigt' ist, und agieren bei der Korrektur und Löschung von veralteten Informationen jenseits der gesetzlichen Regelungen. Generelle Verhaltensregeln und Empfehlungen bei der Ablehnung eines Löschungs- und Aktualisierungswunsches können keine gegeben werden. Ob ein Aktualisierung- bzw. ein Löschungswunsch Erfolgsaussichten hat, muss im Einzelfall analysiert werden. Die ARGE DATEN ist gerne bereit, bei entsprechend gut dokumentierten Fällen zu intervenieren.

LÖSCHEN IM SINNE DER DSGVO

„Löschen" heißt schlicht das Vernichten der Daten im Zusammenhang mit einem bestimmten Zweck und bezieht sich auf jede einzelne Information (Datum). Löschen im Sinne der DSGVO ist keine IT-Funktion und bezieht sich weder auf Datensätze, noch auf Personen, sondern auf konkrete Informationen und Zwecke. Diskussionen wie „physisches" oder „logisches" Löschen sind Scheindiskussionen und ignorieren das eigentliche rechtlich-technische Problem.

Wird eine Information aus verschiedenen getrennt administrierbaren Teilen (Objekten) verwaltet (zB Datenfelder, Datenspalten, ...) dann ist ein Löschungsanspruch je getrennt verwaltetem Objekt zu prüfen und gegebenenfalls das einzelne Objekt zu löschen.

Wird eine Information zu verschiedenen Zwecken verwaltet und einer der Zwecke ist nicht mehr gegeben, dann bedeutet Löschen, das sicherstellen, dass die Information für den nicht mehr zulässigen Zweck nicht mehr verwendet werden kann. Die DSGVO sagt jedoch nichts dazu, wie das ein Verantwortlicher bewerkstelligt. Die Methode muss jedoch so zuverlässig sein, das unter keinen Umständen eine Verarbeitung der Information zu dem nicht mehr zulässigen Zweck möglich ist.

Um zu prüfen, ob „keine Umstände" gegeben sind, empfiehlt es sich typische Ausnahmesituationen zu simulieren und die Wirksamkeit des Löschmanagements zu prüfen:

a. Was passiert im Restorefall?
b. Gibt es Personengruppen mit Sonderrechten, die Zugriff zu den Daten für den nicht mehr zulässigen Zweck erlangen können?
c. Wie ist der gesamte Lifecycle der Daten gestaltet?

Kann unter allen denkbaren Szenarien sichergestellt werden, dass die Daten nicht für den nicht mehr zulässigen Zweck verarbeitet werden können, dann liegt eine korrekte Löschung iS der DSGVO vor. Gibt es überhaupt keinen für den Verantwortlichen vorstellbaren Zweck, dann sind die Daten so zu vernichten, dass keine Person des Verantwortlichen irgendeinen Zugang zu diesen Daten hat. Das wird in der Regel tatsächlich nur durch Vernichten der Datenträger möglich sein.

RECHTE DER BETROFFENEN (KUNDEN)

Betroffene einer Datenanwendung haben das Recht die Löschung ihrer Daten zu beantragen. Bei nichtöffentlichen Datenanwendungen muss dieser Antrag begründet werden. Gründe wären beispielsweise, dass veraltete oder falsche Daten verarbeitet werden oder keine weitere Datenverarbeitung durch das Unternehmen gewünscht ist.

RICHTIGE REAKTION AUF LÖSCHUNGSBEGEHREN

Erhält ein Unternehmen ein Löschungsbegehren, so gilt es festzustellen welche Daten des Betroffenen (Kunden) für welche Zwecke verarbeitet werden. Anschließend gilt es festzustellen für welche Datenverarbeitungen der Verarbeitungszweck durch das Löschungsbegehren weggefallen ist bzw. welche Daten nicht mehr benötigt werden. Nur diese Daten sind zu löschen.

Nicht gelöscht werden müssen Daten die weiterhin einen rechtmäßigen Verarbeitungszweck haben. In vielen Fällen dürfen derartige Daten, aufgrund von gesetzlichen Aufbewahrungspflichten, gar nicht gelöscht werden.

Beispiel: Ein Kunde hat bei einem Unternehmen ein (online) Kundenkonto um über den Webshop zu bestellen oder an einem Bonuspunkteprogramm teilzunehmen. Er entschließt sich nun das Konto zu schließen und seine Daten zu löschen. Was ist zu tun?

Zu beachten ist, dass Daten, die der Kunde beim Erstellen des Kundenkontos angegeben hat, auch für andere Zwecke Verwendung finden können, beispielsweise für die Buchhaltung, das Mahnwesen oder für Marketingzwecke. Es ergeben sich daraus unterschiedliche Situationen.

a. In der Vergangenheit hat der Kunde mehrere Produkte bestellt und unmittelbar bezahlt. Daten über das betriebliche Rechnungswesen müssen sieben Jahre aufbewahrt werden - diese Daten sind daher erst nach Ablauf der Aufbewahrungspflicht zu löschen.
b. Die letzte Rechnung hat der Kunde nicht unmittelbar bezahlt - darum wurde er gemahnt. Diesbezügliche Daten dürfen solange verarbeitet werden bis das Verfahren abgeschlossen ist - oder keine Eintreibung mehr möglich ist. Anschließend sind sie zu löschen.
c. Daten die ausschließlich für die Verwaltung des Kundenkontos verarbeitet werden (Benutzername / Passwort etc.), werden nicht mehr benötigt und sind daher umgehend zu löschen.

SONDERFALL MARKETING

Die Verwendung von Daten zu Marketingzwecken ist ausschließlich für Adressverlage und Direktmarketingunternehmen in § 151 der Gewerbeordnung (GewO) geregelt. Nur diesen gegenüber besteht ein Anspruch auf Löschung bzw. Sperrung.

Bei allen anderen Unternehmen kann ein Betroffener zwar eine Löschung verlangen, er hat jedoch keinen Rechtsanspruch auf

diese. Üblicherweise wird jedoch derartigen Löschungswünschen stattgegeben. Es könnte jedoch ein Unternehmen auf dem Standpunkt stehen, jemand der JETZT keine Werbezusendung will, könnte zukünftig, etwa auf Grund geänderter Alters- oder Einkommensverhältnisse, seine Meinung ändern.
Beachtet werden müssen die Bestimmungen des Telekommunikationsgesetzes (TKG 2003) bezüglich der elektronischen Werbung.

MITTEILUNGS- UND INFORMATIONSPFLICHT DES VERANTWORTLICHEN

Besteht die Berichtigungs- oder Löschungspflicht, so sind alle Empfänger von Daten über die Löschung oder die Berichtigung zu informieren (Art. 19 DSGVO). Die DSGVO normiert damit auch eine umfassende Mitteilungspflicht.

Falls der Verantwortliche die personenbezogenen Daten von Betroffenen veröffentlich hat und zur Löschung verpflichtet ist, sind auch Informationspflichten zu beachten. Er muss alle Datenempfänger über das Löschungsbegehren des Betroffenen unterrichten.

FRISTEN

Auf Berichtigungen und Löschungen muss grundsätzlich gemäß Art 17 DSGVO unverzüglich (ohne schuldhaftes Zögern), spätestens aber binnen eines Monats auf das Begehren des Betroffenenhin, reagiert werden. Entweder muss diesem mitgeteilt werden, dass dem Antrag entsprochen wurde oder es muss schriftlich begründet werden, warum das Begehren nicht durchführbar ist.

BESCHWERDE- UND SCHADENERSATZRECHT

Wenn der Verantwortliche einem Löschungsbegehren des Betroffenen nicht nachkommt, dann besteht die Beschwerdemöglichkeit bei der Datenschutzbehörde. Die Verletzung des Löschungs- und Berechtigungsrechts wird mit bis zu EUR 20 Mio., oder bei Unternehmen mit bis zu 4% des letzten weltweiten Jahresumsatzes bestraft (Art 83 Abs 5 DSGV0). Die Höchstrichter werden in Zukunft darüber entscheiden, wie hoch die Strafen tatsächlich sein werden. Weiteres hat der Kunde das Recht auf Schadenersatz, sofern ein materieller oder immaterieller Schaden entstanden ist (Art 82 DSGVO). Für Schadenersatzklage gemäß Art 16 und 17 DSGVO sind die Landesverwaltungsgerichte (nicht die Datenschutzbehörde) zuständig.

LESEN VON E-MAILS DER MITARBEITER DURCH DIE FIRMENLEITUNG

Grundsätzlich fallen E-Mails wie traditionelle Poststücke unter den weiten Begriff des Art 8 der Europäischen Menschenrechtskonvention (EMRK) und sind als Teil der „Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs“ anzusehen.

Zu beachten ist jedoch, dass der rechtliche Begriff ‚Briefgeheimnis‘ vom OGH eng ausgelegt wird. Grundsätzlich fallen nur verschlossene Briefe unter das Briefgeheimnis und sind durch Art 10 Staatsgrundgesetz (StGG) besonders geschützt. Um die technischen Probleme bei elektronischen Nachrichten zu umgehen, wurde 1975 mit Art 10aStGG eine Sonderbestimmung für elektronisch übermittelte Nachrichten geschaffen: „Das Fernmeldegeheimnis darf nicht verletzt werden. Ausnahmen von der Bestimmung des vorstehenden Absatzes sind nur auf Grund eines richterlichen Befehles in Gemäßheit bestehender Gesetze zulässig.“

Aus dieser Differenzierung „normaler“ und elektronischer Post ergeben sich auch unterschiedliche strafrechtliche Konsequenzen. Die Verletzung des Briefgeheimnisses im engeren Sinn ist gemäß § 118 Strafrechtsgesetzbuch (StGB) zu verfolgen, bei Verletzungen des Telekommunikationsgeheimnisses (etwa E-Mails, Telefonate, ...) gemäß § 119 StGB.

Zusätzlich bestehen Strafbestimmungen gemäß § 93 Telekommunikationsgesetz (TKG 2003) (Verletzung des Kommunikationsgeheimnisses), wenn die Verletzung durch einen Betreiber eines Kommunikationsdienstes (bzw. seine Mitarbeiter) erfolgte.

Weiteres ergeben sich verschiedene andere rechtliche Bestimmungen zur Geheimhaltung von E-Mails. Zuerst ist der Schutz von Daten gemäß Art 1 DSGVO zu nennen, aber auch Bestimmungen des Allgemeinen Bürgerlichen Gesetzbuches (ABGB) oder des Urhebergesetzes (UrhG) kommen in Frage.

PRAKTISCHE AUSLEGUNGS- UND ANWENDUNGSPROBLEME

Grundsätzlich ist von einer Geheimhaltung von E-Mails auszugehen, egal welcher der Aspekte, Privatsphäre (zB § 16, § 1328a ABGB), Datenschutz (zB Art 1 DSGVO), Telekommunikationsrecht (zB § 93 TKG 2003), Arbeitsrecht (zB § 96, § 96a ArbVG), Strafrecht (zB §§ 118, 119 StGB), Urheberrecht (zB § 77 UrhG), im Einzelfall überwiegen wird.
Aktuelle Version der gesetzlichen Bestimmungen siehe http://www.ris2.bka.gv.at/bundesrecht/.

Alle diese Geheimhaltungsbestimmungen können aus verschiedensten Gründen relativiert werden (etwa zum Zweck der Strafverfolgung, wegen überwiegender Interessen Dritter usw.).

Leider hat es der Gesetzgeber verabsäumt, eine klare und zumindest begrifflich einheitliche Linie in die Kommunikationsregeln zu bringen. So wird an einer Stelle vom „Briefgeheimnis“ (§ 118 StGB, Art 10 StGG), dann vom „Fernmeldegeheimnis“ (Art 10a StGG), dem „Telekommunikationsgeheimnis“ (§ 119 StGB), dem „Kommunikationsgeheimnis“ (§ 93 TKG 2003) gesprochen, an anderer Stelle nur von „ähnlichen vertraulichen Aufzeichnungen“ (§ 77 UrhG). Zum Teil werden idente, zum Teil unterschiedliche Sachverhalte beschrieben.

In Hinblick auf die zunehmende Konvergenz der verschiedenen Kommunikationsmittel scheint eine rechtliche Generalsanierung dieses wichtigen Bereiches als sinnvoll. Mit der Einführung der Begriffe „Kommunikation“, „Kommunikationsgeheimnis“ und „Kommunikationsmittel“ könnten alle Formen des Informationsaustausches geregelt und auf gleichem Niveau geschützt werden. Leider ist eine derartige Vereinheitlichung nicht in Sicht.

Durch das Kommunikationsgeheimnis geschützt sind E-Mails vor der Einsichtnahme / Verwertung durch unberechtigte Dritte. Geschützt sind dabei sowohl die Geheimhaltungsinteressen des Absenders, des Empfängers und jener Personen, die im E-Mail genannt werden.

Nun wird bei einem betrieblich veranlassten E-Mail grundsätzlich davon auszugehen sein, dass der berechtigte Empfänger das Unternehmen selbst ist und der konkrete Bearbeiter des E-Mails als Organ des Unternehmens tätig ist. Damit ergibt sich grundsätzlich auch das Recht des Unternehmens - abhängig von seiner internen Organisation - dass alle berechtigten Organe ein einlangendes dienstliches E-Mail lesen dürfen.

Wer ein berechtigtes Organ ist, muss durch Dienstanweisungen, Organisationsrichtlinien usw. vorab so geklärt sein, dass der einzelne Benutzer eines E-Mail-Accounts weiß was mit seinen dienstlichen Mails passiert (Archivierung, Kopien, Lesezugriffe durch Dritte).

Kein Anspruch auf Verwertung (Lesen durch Dritte, Archivierung, Kopieren) hat jedoch ein Unternehmen bei E-Mails mit privatem Inhalt. Selbst wenn ein Unternehmen seinen Mitarbeiter verbietet, private E-Mails über Firmen-Accounts zu versenden, kann das Unternehmen es nicht beeinflussen, dass ein Mitarbeiter ein privates E-Mail erhält. Dieses E-Mail darf das Unternehmen (bzw. seine Organe) „nicht zur Kenntnis nehmen", unabhängig welche internen Organisationsrichtlinien gelten.

Der Schutz des gesetzlich garantierten Kommunikationsgeheimnisses wiegt schwerer als innerorganisatorische Richtlinien.

Damit ergeben sich praktische Umsetzungsprobleme für das grundsätzliche Recht des Unternehmens betriebliche E-Mails durch verschiedene Personen zu lesen bzw. Kopien anzufertigen. In vielen Fällen ist bei einem E-Mail von außen nicht erkennbar, ob es dienstlichen oder privaten Charakter hat. Im Allgemeinen wird daher über den Account-Inhaber hinaus niemand die E-Mails lesen. Begründete Abweichungen von dieser Praxis, etwa unvorhergesehene Verhinderung des berechtigten Account-Inhabers, Gefahr in Verzug, konkreter Verdacht rechtswidriger Tätigkeiten usw. müssen daher vorher geregelt werden.

KEIN GENERELLER BETRIEBLICHER LESEANSPRUCH

Ob Vorgesetzte, Betriebsinhaber oder sonstige betriebliche Bevollmächtigte (zB externe IT-Spezialisten) E-Mails lesen dürfen oder nicht, hängt von der Art der Mails, Vereinbarungen mit den Mitarbeitern und Weisungen an die Mitarbeiter ab. Dabei können drei Fälle unterschieden werden.

1) BETRIEBLICHE E-MAILS
Dass die Geschäftsführung betriebliche E-Mails (Kontakt mit Kunden, Geschäftspartnern, etc.) lesen darf, wenn Mitarbeiter in Urlaub oder krank sind oder nachdem diese das Unternehmen verlassen haben, ist zulässig und bedarf keiner gesonderten Vereinbarung.

2) PRIVATE E-MAILS
Die Kenntnisnahme privater Kommunikation ist jedenfalls unzulässig. Lässt die Absende- oder Empfänger-Adresse, der Betreff oder der Inhalt einer E-Mail auf privaten Charakter schließen, so darf diese E-Mail nicht zur Kenntnis genommen werden.

Es empfiehlt sich mit den Mitarbeitern klare Regeln über die private Nutzung von E-Mail-Postfächern zu vereinbaren. Wird zB das Empfangen und Verschicken privater E-Mails zumindest geduldet, dann wird ein generelles Lesen von E-Mails durch Dritte nicht zulässig sein. Wird beides ausdrücklich untersagt, ist der Geheimnisschutz wesentlich schwächer ausgeprägt, weil dann auch nur geschäftliche E-Mails vorhanden sein dürften. Zu beachten ist jedoch, dass der Empfang von privaten E-Mails nicht vollständig „verboten" werden kann, da der Empfänger keinen Einfluss darauf hat, wer ihn Nachrichten zuschickt.

3) SONSTIGE E-MAILS
Sollen E-Mails aber zu anderen als betrieblichen Zwecken untersucht werden, etwa, um unternehmensschädigendes Verhalten von Mitarbeitern festzustellen, zu Schulungszwecken oder Sonstigem, muss dies mit den Mitarbeitern vereinbart sein.

BETRIEBSVEREINBARUNGEN, VERTRAGLICHE VEREINBARUNGEN, GESETZLICHE BESTIMMUNGEN

In allen drei Fällen sind allgemeine Vereinbarungen mit Mitarbeitern zu beachten. In der Regel wird das ArbVG (§ 96 bzw. § 96a) zu berücksichtigen sein: Überwachungsmaßnahmen, die die Menschenwürde berühren bzw. sonstige Aufzeichnungen werden einer Zustimmung des Betriebsrats bedürfen.

Individuelle Vereinbarungen mit einzelnen Mitarbeitern dürfen dabei einer allgemeinen Betriebsvereinbarung nicht widersprechen. Eingriffe in Mitarbeiter-E-Mail-Accounts sollten daher nur auf Basis konkreter Vorgaben möglich sein und nach dem Vier-Augen-Prinzip erfolgen (zB Geschäftsführung gemeinsam mit Betriebsrat, wo dieser fehlt mit einer Vertrauensperson oder einer rechtskundigen Person).

Ist im Zuge einer derartigen Einschau der private Charakter eines E-Mails erkennbar, darf es nicht weiter „zur Kenntnis genommen" werden, eine Verwertung durch das Unternehmen, Vorgesetzte oder Organe des Unternehmens ist unzulässig.

VERHALTEN BEI VERDACHT STRAFRECHTLICH RELEVANTEN HANDELNS

Selbst bei Vorliegen eines konkreten Verdachts, ein bestimmter Mitarbeiter würde gegen Bestimmungen des Strafgesetzes verstoßen, ist ein Lesen von E-Mails ohne entsprechende Vereinbarung oder der Zustimmung des Betroffenen unzulässig.

Verstöße gegen das Strafgesetz sind beispielsweise das Verletzen von Geschäfts- oder Betriebsgeheimissen, das widerrechtliche Zugreifen auf ein Computersystem, die Datenbeschädigung, aber auch eine Datenverwendung mit Gewinn- oder Schädigungsabsicht (§ 63 DSG).

In derartigen Fällen darf der E-Mail-Verkehr des Mitarbeiters zwar nicht gelesen, jedoch forensisch gesichert und im Rahmen

einer Strafanzeige an Strafbehörden übermittelt werden. Gegen den Mitarbeiter muss allerdings ein konkreter, belegbarer Verdacht vorliegen. Bloße Annahmen rechtfertigen das Übermitteln der E-Mails nicht. Konkrete Hinweise, dass ein Mitarbeiter zB Geschäftsgeheimnisse verrät, wären beispielsweise, dass Mitbewerber ihre Preise oder Produkte ähnlich gestalten. Werden E-Mails ohne entsprechende Vereinbarung unbefugt gelesen, wird dadurch gegen das Telekommunikationsgeheimnis (§ 119 StGB) verstoßen.

MINDESTMASS AN PRIVATSPHÄRE AUCH IN UNTERNEHMEN

Das generelle Lesen von allen Mails aller Mitarbeiter ist in den meisten Fällen nicht zulässig. Das Lesen der Geschäftspost ist selbst ohne besondere Vereinbarung zulässig, private Kommunikation darf generell nicht zur Kenntnis genommen werden. Sollen E-Mails zu anderen als betrieblichen Zwecken ausgewertet werden (Missbrauchserkennung), bedarf dies einer Vereinbarung mit den Mitarbeitern. Einen konkreten Verdacht vorausgesetzt dürfen E-Mails aber zur Anzeige an Strafbehörden übermittelt werden.

DAS RECHT AUF DATENÜBERTRAGUNG (DATENPORTABILITÄT)

Durch die Datenschutz-Grundverordnung (DSGVO) wurde das neue Betroffenenrecht ‚Datenübertragbarkeit' eingeführt. Dieses Recht soll die Übertragung von personenbezogenen Daten, die Betroffene einem verantwortlichen Verarbeiter bereitgestellt haben, an einen neuen Verantwortlichen erleichtern. Zusätzlich soll ein Betroffener dadurch mehr Kontrolle über die eigenen Daten erhalten.

DAS RECHT PERSONENBEZOGENE DATEN ZU ERHALTEN

Im Zuge eines Geschäftsprozesses übermittelt der Kunde (Betroffener) seine personenbezogenen Daten an den Verarbeiter/Unternehmer (Verantwortlicher). Der Verantwortliche ist gemäß Art 20 DSGVO verpflichtet, die bereit gestellten Daten auf Verlangen elektronisch an den Betroffenen zu übermitteln. Zusätzlich müssen Betroffene vorab über das Bestehen dieses Rechts gemäß Art 13 und 14 DSGVO in Kenntnis gesetzt werden.

Die Herausgabepflicht der Daten durch den Verantwortlichen ermöglicht zunächst die private Nutzung der Daten für den Betroffenen. Beispielsweise kann der Betroffene die Daten per E-Mail erhalten. Diese Möglichkeit bringt viele praktische Vorteile für den Betroffenen. So kann er beispielsweise alle Kontakte aus seinem Webmail-Dienst abrufen, um eine Neujahrs-Glückwunschliste zu erstellen. Weiters kann die betroffene Person ihre Film Play List bei einem Video-Streaming-Dienst abrufen, damit ein Doppelkauf auf einer anderen Online-Plattform verhindert wird.

Die Bestimmung sieht keine branchenspezifischen oder inhaltlichen Einschränkungen vor. Im Extremfall sind auch Onlineservices denkbar, bei denen sich ein Betroffener einmalig mit seinen wesentlichen Stammdaten registriert (Name, Anschrift, Geburtsdaten, Kontodaten, ...) und in Zukunft dieses Service beauftragt seine Daten an andere Verantwortliche zu übermitteln.
Beschränkt ist das Recht auf Datenübertragung ausschließlich dadurch, dass nur die vom Betroffenen bereit gestellten Daten übertragen werden müssen, NICHT jedoch die Daten, die der Verantwortliche selbst generiert, etwa Auswertungen, Verbrauchsdaten, Abrechnungsdaten, Vertragsdaten, ...

BEISPIELE ZUR DATENPORTABILITÄT

Zu denken ist an eine Übertragung der Telefonkontaktdaten im Zuge eines Wechsels des Mobilfunk-Diensteanbieters. Der neue Verantwortliche kann alle Mobilnummern unter Einhaltung der Vorschriften des Art 6 DSGVO verarbeiten.

Eine ähnliche Situation liegt vor, wenn ein Bankkunde seine Hausbank wechselt. Im Zuge dessen beantragt er die Übertragung der personenbezogenen Daten gemäß Art 20 DSGVO. Dabei werden Datensätze über die Käufe und Transaktionen des Kontoinhabers übermittelt.

Andere Bereiche in denen die Datenübertragung von Bedeutung sein kann:

- Social Media (Übertragung von Postings, Bildern, Interessen, Profilen, ...)
- Cloud-Service (Übertragung alle hochgeladenen Daten, ...)
- Datingplattformen (Übertragung der eigenen Personenangaben und Partnerpräferenzen)
- Online-Shops (Übertragung von Bestelldaten, Produktpräferenzen, ...)
- Universität (Übertragung der inskribierten Lehrveranstaltungen, ...)
- Suchmaschinen (Übertragung der Suchanfragen, ...)
- Navigationsgeräte (Übertragung der gespeicherter Routen,...)

ÜBERMITTLUNG AN NEUE VERANTWORTLICHE

Gemäß Art 20 DSGVO haben Betroffene das Recht auf Übermittlung der personenbezogenen Daten vom bisherigen Verantwortlichen an einen neuen Verantwortlichen.

Der neue Verantwortliche hat die Vorschriften des Art 5 DSGVO einzuhalten. Somit sind nur für den Zweck der neuen Verarbeitung erforderliche Daten zu speichern. Der Zweckbindungsgrundsatz besagt, dass personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden müssen.
Insofern muss der neue Geschäftspartner die Löschung der überschüssigen Daten veranlassen. Das Recht auf Datenübertragbarkeit erleichtert dem Betroffenen somit den beliebigen Wechsel zwischen Dienstanbietern.

Beispielsweise hat ein Betroffener seine Kündigung bei seinem alten Stromlieferanten veranlasst. Im Zuge dessen hat er eine neue Vereinbarung mit einem anderen Stromanbieter abgeschlossen. Mit dieser Kündigung hat der Betroffene zugleich die Datenübermittlung an den neuen Geschäftspartner beantragt. Durch die direkte Übermittlung der personenbezogenen Daten wie zum Beispiel Namen, Adresse, E-Mail, Geburtsdatum, Bankdaten, etc. soll der Betroffen Zeit sparen, indem er seine Daten nicht selbst übermitteln muss.

BEACHTUNG DER RECHTE DRITTER

Im Zuge der Datenübertragung an den neuen Verantwortlichen können grundsätzlich auch personenbezogene Daten Dritter enthalten sein.

Sowohl der ursprüngliche Verantwortliche, als auch der neue Verantwortliche sind verpflichtet die Rechte Dritter zu beachten. Eine generelle Weigerung die Daten Dritter zu übertragen wird jedoch nicht zulässig sein.
Der ursprünglich Verantwortliche wird jedoch Nachweise beim Betroffenen verlangen können, dass diese Dritten (zB Angehörige, Freunde, ...) dieser Übertragung zugestimmt haben oder aus anderen Gründen die Übertragung zulässig ist.

FORMVORSCHRIFT, FRIST UND ENTGELTLEISTUNG

Das Anspruchsbegehren des Betroffenen auf Datenübertragung kann formlos erfolgen und der Verantwortliche muss unverzüglich, in jedem Fall aber binnen eines Monats, den Antrag erledigen. In Ausnahmefällen und mit Begründung, beispielsweise bei komplexen Anträgen, hat der Verantwortliche zwei weitere Monate Zeit. Aus dem Recht auf Datenübertragbarkeit dürfen dem Betroffenen keine Kosten entstehen. Zahlungspflicht des Betroffenen entsteht nur bei offenkundig unbegründeten oder aufgrund ihrer Häufigkeit exzessiven Anträgen.

Grundsätzlich erfolgt die Herausgabe und Übertragung der Daten an den neuen Geschäftspartner gemäß Art 20 DSGVO im Rahmen einer Einwilligung des Betroffenen. Weiters kann auch die Datenübertragung mittels einer Vereinbarung zwischen dem Betroffenen und dem neuen Verarbeiter erfolgen. Für Datenübermittlungen mit personenbezogenen Daten Dritter muss ein weiterer Grund, wie zum Beispiel Art 6 DSGVO, für die Rechtmäßigkeit vorliegen.

Das Recht auf Datenübertragung kann nicht gegenüber Auftragsverarbeitern geltend gemacht werden.

WANN WERDEN PERSONENBEZOGENEN DATEN VOM BETROFFENEN BEREITGESTELLT?

In den Anwendungsbereich der Datenübertragbarkeit fallen primär personenbezogene Daten des Betroffenen. Der Anspruch erstreckt sich auch auf pseudonymisierte Daten, wenn die Identifizierung des Betroffenen möglich ist, nicht hingegen auf anonymisierte Daten oder Daten Dritter.

Neben Stammdaten fallen auch Daten, die der Betroffene im Zuge eines Dienstes bekannt gegeben hat darunter, zum Beispiel Suchanfragen oder Navi-Daten, Eingaben auf Fitness- oder Gesundheitsgeräten.

Auswertungen anhand von Betroffenen bereit gestellten Daten sind von Art 20 DSGVO ausgenommen. Typische Beispiele Bonitätsbewertungen oder diagnostische Ergebnisse.

Ungeklärt ist derzeit, ob auch Daten, die durch Aktivitäten des Betroffenen erzeugt werden, ebenfalls unter den Begriff „vom Betroffenen bereit gestellt" fallen. Dies wären Aufzeichnung bei medizinischen Geräten, bei Fitnessgeräten, bei Freizeittrackern oder jede sonstige Form von Geo-Location.

FORM DER ELEKTRONISCHEN ÜBERMITTLUNG UNGEKLÄRT

Die personenbezogenen Daten müssen vom bisherigen Verantwortlichen so zur Verfügung gestellt werden, dass der Betroffene oder der neue Verantwortliche sie einfach übernehmen kann.

Die DSGVO sieht dazu jedoch keinerlei technische Vorgaben vor. Im Ergebnis werden es XML-Datenstrukturen sein. Es ist jedoch zu hoffen, dass diesbezüglich rasch Rechtssicherheit geschaffen wird.

GELDSTRAFE UND SCHADENERSATZ

Ein Betroffener kann bei Rechtsverletzung eine Beschwerde bei der Datenschutzbehörde einreichen. Ein Verstoß gegen das Recht auf Datenübertragbarkeit kann gemäß Art 83 DSGVO mit bis zu EUR 20 Mio. oder bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres bedroht.

Weiteres hat der Betroffene wegen Verstoß gegen die Bestimmung gemäß Art 21 DSGVO Recht auf Schadenersatz, sofern ein materieller oder immaterieller Schaden entstanden ist. Ein materieller Schaden entsteht, wenn der Verantwortliche keine personenbezogenen Daten im geeigneten Format bereitstellt, obwohl der Betroffene bereit war diese zu empfangen und er dadurch einen zusätzlichen Erhebungsaufwand hat.

Ein immaterieller Anspruch kann wohl schon allein dadurch entstehen, als dem Betroffenen Grundrechte verwehrt werden. Zum gegenwärtigen Zeitpunkt kann aber weder Spruchpraxis, noch Höhe des zugesprochenen Schadenersatzes abgeschätzt werden.

Für Schadenersatzklagen gemäß Art 21 DSGVO sind die ordentlichen Gerichte (nicht die Datenschutzbehörde) zuständig. Der Betroffene kann die Klage entweder beim Gericht, in dessen Sprengel er seinen gewöhnlichen Aufenthalt oder Sitz hat oder beim Landesgericht erheben, in dessen Sprengel der Verantwortliche seinen gewöhnlichen Aufenthalt, Sitz oder eine Niederlassung hat.

VERÖFFENTLICHEN VON SCHULBESUCHSDATEN IM INTERNET

DSGVO ART 1, 4, 5, 6
Information, ob die Veröffentlichung von biographischen Schülerdaten im Internet laut Datenschutzgrundverordnung erlaubt ist - Zweck - Beschaffung - Folgen

Sowohl Schulen, als auch Absolventenverbände, Elternvereine und (ehemalige) Schüler fragen regelmäßig an, ob die Veröffentlichung von biographischen Schülerdaten auf einem Schulwebserver oder auch einem privaten Webserver eines Elternvereins oder eines Schülers veröffentlicht werden dürfen.

Als grundsätzliche Vorbemerkung gilt: auch Schulbesuchsdaten (wer, wann, welche Schule, mit welchem Erfolg absolviert hat) fallen als persönliche Informationen unter die Datenschutzgrundverordnung (DSGVO) gemäß Art 4. Das verwenden dieser Informationen durch Dritte (Freunde, Verwandte, Schule, Behörden oder Arbeitgeber) stellt einen Eingriff in die Privatsphäre gemäß Art 1 DSGVO dar und ist daher mit dem Betroffenen gemäß Art 6 DSGVO abzustimmen.

Tatsächlich sind viele Menschen interessiert, dass Informationen über sie veröffentlicht werden. Umgekehrt ist jedoch der Wunsch einzelner Personen auf Anonymität und Achtung Ihrer Privatsphäre zu respektieren.

Unter Bedachtnahme dieser Grundsätze sind zwei Aspekte zu analysieren:
1. Zu welchem Zweck werden die Schulbesuchsinformationen verwendet?
2. Wurden die einzelnen Informationen (der Schüler) rechtmäßig ermittelt?

1. KLÄRUNG DES ZWECKES:
Der Zweck einer Datenverwendung gemäß Art 5 DSGVO kann sich aus Gesetzen, wie dem Schulunterrichtsgesetz ergeben, aber auch aus den Vereinsstatuten (Elternverein, Absolventenverband). In der Regel fällt es nicht unter die Aufgaben der Schulen, Biographien von ehemaligen Schülern zu verwalten und zu veröffentlichen. Daher wird eine Schule, unabhängig von der Zustimmung des Betroffenen, NICHT berechtigt sein, Absolventendaten

‚ins Internet' zu stellen. Ein Absolventenverein kann jedoch dazu berechtigt sein und wird Biographien ehemaliger Schüler ins Internet stellen dürfen. Ebenso wird dies eine Privatperson können, wenn es sich um seine ehemaligen ‚Schulfreunde' handelt.

2. BESCHAFFUNG DER DATEN:
Auch, wenn es die statutenmäßige Aufgabe eines Absolventenverbandes ist, Biographien im Internet zu veröffentlichen, benötigt er für die tatsächliche Veröffentlichung von jedem betroffenen Schüler die Zustimmung. Gleiches gilt bei der privaten Veröffentlichung gemäß Art 6 DSGVO. Diese Zustimmung kann dann entfallen, wenn die verwendeten Informationen vorher schon zulässig veröffentlicht wurden (etwa bei bekannten Persönlichkeiten) und der frühere Zweck der Veröffentlichung mit dem neuen Zweck, im Wesentlichen, übereinstimmt.

Wenn also eine Information in einem Telefonbuch veröffentlicht wurde, mit dem Zweck diese Person anrufen zu können oder sie benachrichtigen zu können, wird man diese Daten, etwa die Telefonnummer nicht auf eine Kontaktanzeigenseite schreiben dürfen, mit der Aufforderung, diese Person anzurufen. Auch die Veröffentlichung im Zusammenhang mit einem abgeschlossenen Schulbesuch wird nicht zulässig sein.

Um sicher zu gehen, dass bei der Erstellung einer Absolventen-Web-Seite die Privatsphäre der betroffenen Personen nicht verletzt werden, sollte man die Zustimmung aller betroffenen Personen einholen.

FOLGEN BEI NICHTEINHALTUNG

Wird ein Betroffener in seiner Privatsphäre persönlich verletzt, kann er gegen den Datenverarbeiter Beschwerde erheben. Die Nichteinhaltung des Zweckbindungsgrundsatzes gemäß Art 5 DSGVO und des Gebots der rechtmäßigen Verarbeitung gemäß Art 6 DSGVO kann mit einer Strafe bis zu 20 Millionen Euro oder im Falle eines Unternehmens mit bis zu 4% des weltweiten Jahresumsatzes gerechnet werden, je nach dem was höher ist. Außerdem kann ein Betroffener Schadenersatz für die Rechtsverstöße gegen die Bestimmungen des Art 5 und 6 DSGVO geltend machen.

AUSKUNFTSRECHT BEI PSEUDONYMEN DATEN GEMÄSS DSGVO (FACEBOOK, GOOGLE UND CO)

DSGVO Art 5, 11, 15
Sonderregelung für Identifizierung der betroffenen Person - Entfall des Auskunftsrechts im besonderen Fall - Löschungspflicht der Identifizierungsdaten - Auskunftsrecht auch bei pseudonymisierten Daten

Nach dem alten DSG 2000 musste nur Auskunft bei identifizierten Datenverarbeitungen, etwa bei einem Bankkonto, einem Kundenkonto, einem Patientenakt oder aus der Wählerevidenz, gegeben werden. Mit der DSGVO (ab 25.5.2018) MUSS auch bei sonstigen personenbezogenen Verarbeitungen Auskunft gegeben werden, wenn der Betroffene ausreichend mitwirkt und auf Grund der Mitwirkung bestimmt werden kann.

VARIANTE A: GOOGLE-SUCHE MIT BESTEHENDEM GOOGLE-KONTO

Grundsätzlich hat jeder Internetnutzer die Möglichkeit Google Produkte und Dienste zu nutzen. Für eine identifizierte Google-Nutzung muss ein Google-Konto existieren. Für die Registrierung eines Google-Accounts sind folgende personenbezogene Daten erforderlich: Name, Geburtsdatum, Geschlecht, E-Mail, Telefonnummer und Passwort. Auf diese Weise werden die Daten des Betroffenen identifizierbar verarbeitet. Folglich ist eine pseudonymisierte Datenverarbeitung ausgeschlossen.
Das Recht auf Auskunft hat im Datenschutzbereich eine wesentliche Bedeutung. Die Bestimmungen der DSGVO legen genau fest, in welcher Art und Weise einer betroffenen Person Auskunft erteilt wird.
Die grundsätzlichen Voraussetzungen für das Auskunftsbegehren und die Auskunftserteilung sind im Art 12 und Art 15 DSGVO geregelt. Gemäß Art 15 DSGVO erhält der Betroffene in erster Linie Auskunft über die laufenden Verarbeitungen von personen-

bezogenen Daten und die Zwecke für die Datenverarbeitung. Der Verantwortliche hat gemäß Art 12 DSGVO zu gewährleisten, dass die Auskunft grundsätzlich schriftlich, fristgerecht und kostenlos erfolgt.

Infolge dieser Bestimmungen hat ein Google-Kontoinhaber als Betroffener einen Auskunftsrechtsanspruch. Weiteres hat Google als Verantwortlicher alle Anforderungen der DSGVO einzuhalten. Vor allem darf er die Betroffenenrechte gemäß Art 15 bis 20 DSGVO seiner Kontoinhaber nicht verletzen. Damit verpflichtet ein Auskunftsansuchen eines Google-Kontonutzers den Verantwortlichen zur Verschaffung von Informationen.

VARIANTE B: GOOGLE-SUCHE OHNE GOOGLE KONTO (PSEUDONYMISIERTE SUCHE)

Der Zugang zum Internet wird per IP-Adressen hergestellt, Google verwendet zusätzlich eine Reihe weiterer Tracking-Methoden, um seine Nutzer eindeutig zu bestimmen, den Ort des Nutzers zu ermitteln, sein Verhalten über eine längere Zeit zu verfolgen etc. Targeting, Tracking und Nudging sind die Big-Data-Technologien, die Google einsetzt.

Neben der IP-Adresse bedient sich Google auch der Computereinstellungen des Benutzers (die sogenannte Computer-Signatur), der installierten Browser-Fonts, installierter Plugins und Cookies, um personenbezogene Informationen zu protokollieren.

Diese Art von Internetnutzung erfolgt in der Regel auf Basis pseudonymisierter Datenverarbeitung, da primär die IP-Adresse, die Interneteinstellung, die Cookies und keine anderen Identifizierungsmerkmale des Nutzers in Betracht kommen. Selbst wenn der Benutzer Standort oder IP-Adresse wechselt, seine Cookies löscht oder seinen Browser wechselt, kann der Benutzer noch immer identifiziert werden (getrackt werden). Nur wer alles ändert, hat die Chance als „neuer" Benutzer bei Google aufzuscheinen.

SPEICHERUNG DER IDENTIFIZIERUNGSDATEN ENTFÄLLT

Gemäß Art 11 Abs 1 DSGVO sind ‚Verarbeitungen, in denen eine Identifizierung der Betroffenen nicht oder nicht mehr erforderlich ist', besonders geregelt. Auf Grundlage dieser Sonderbestimmung sind Verantwortliche nicht verpflichtet die Identifizierungsdaten der Betroffenen, ‚zur bloßen Einhaltung der Vorschriften der DSGVO', aufrechtzuhalten. Zum Beispiel bei der Pseudonymisierung, d.h. ein Name oder ein anderes Identifikationsmerkmal wird durch ein Kennzeichen ersetzt wird. Dadurch wird die Identifizierung der betroffenen Personen ausgeschlossen oder wesentlich erschwert. So müssen die Betroffenenrechte gemäß Art 15 bis 20 DSGVO nicht eingehalten werden.

Angesichts dieser Punkte darf Google pseudonymisierte Datenverarbeitung gemäß Art 11 Abs. 1 DSGVO vornehmen. Alle Google-Konto Inhaber verlieren dadurch grundsätzlich Ihre Betroffenenrechte, insbesondere das Auskunftsrecht.

WAHRNEHMUNG DER BETROFFENENRECHTE, INSBESONDERE AUSKUNFTSRECHT

Der Einzelne kann jedoch seine Betroffenenrechte gemäß Art 15 bis 20 DSGVO sichern, indem er weitere personenbezogene Daten zur Verfügung stellt, um seine Identität offen zu legen. Die Sonderregelung des Art 11 Abs 2 DSGVO ermöglicht somit ein Recht auf Auskunft gemäß Art 15 DSGVO.

Gemäß Art 11 Abs 2 können auch Google-Nutzer, bei einfacher Internetnutzung (ohne Google-Account), Ihre Betroffenenrechte in Anspruch nehmen. Durch die Angabe weiterer personenbezogenen Daten, zB den Namen, ist die pseudonymisierte Datenverarbeitung ausgeschlossen. Die Identifizierung des Google-Nutzers ist dadurch erfüllt.

DAS GEBOT DER ZWECKBINDUNG

Bei der Datenverarbeitung muss gemäß Art 5 Abs 1 lit e DSGVO geprüft werden, ob eine Identifizierung der betroffenen Person für die Verarbeitungszwecke notwendig ist.

Diese Prüfpflicht sieht vor, dass Daten nur so lange gespeichert werden dürfen, wie es für die Verarbeitungszwecke erforderlich ist. Google ist grundsätzlich berechtigt/verpflichtet die Identifizierungsdaten zu speichern, solange die Identifizierbarkeit seiner Kunden für die Verarbeitungszwecke erforderlich ist. Beispielsweise muss Google als Verantwortlicher die Datenschutzbestimmungen der DSGVO einhalten, wenn ein Betroffener das Google-Konto besitzt.

LÖSCHUNG DER IDENTIFIZIERUNGSDATEN

Um das Gebot der Datenminimierung gemäß Art 5 Abs 1 lit c DSGVO und der Speicherbegrenzung des Art 5 Abs 1 lit e DSGVO zu erfüllen, muss ein Verantwortlicher Identifikationsdaten so früh als möglich löschen.

Wenn ein ehemaliger Google-Kontoinhaber seinen Account unwiderruflich löscht, dann erfolgt in der Regel die zukünftige Nutzung von einfachen Google Diensten nur anhand der IP-Adresse (und sonstigen Tracking-Daten) in Form der pseudonymisierten Datenverarbeitung. So darf Google keine personenbezogene Datenverarbeitung in identifizierender Weise vornehmen.

NACHWEIS DER NICHTIDENTIFIZIERBARKEIT

Wenn im Zuge eines Auskunftsbegehrens - trotz Vorlage von Identifikationsdaten durch den Betroffenen - festgestellt wurde, dass eine Identifizierung des Betroffenen nicht möglich ist, so hat der Verantwortliche die betroffene Person darüber zu informieren. Strittig ist, ob diese Information auch eine Begründung enthalten muss oder ob die Nachricht reicht, dass zum Betroffenen mit seinen Angaben keine personenbezogenen Daten identifiziert werden konnten.

Eine Identifikation wäre jedoch schon gegeben, wenn Google beispielsweise über eine eMail Adresse oder eine Kontaktnummer verfügt, die der Betroffene bekannt gibt und mit deren Hilfe Google weitere Informationen (zB Suchanfragen der letzten Wochen) verknüpft.

AUSKUNFTSANSPRUCH GILT AUCH FÜR ANDERE PSEUDONYMISIERTE VERARBEITUNGEN

Selbstverständlich besteht dieser Auskunftsanspruch auch gegenüber jedem anderen Verarbeiter der pseudonymen Verarbeitungen vornimmt.

So betreibt der österreichische Versicherungsverband eine KFZ-Schadensdatenbank, in der Schadensfälle zu KFZs gespeichert sind. Unter anderem Art und Höhe der Schäden. Informationen, die für den Käufer eines Gebrauchtwagens geradezu Gold wert sein können, bisher aber nicht bekannt gegeben wurden.

Die Verwaltung der Daten erfolgt durch Speicherung der Seriennummer des KFZs. Ist jemand Inhaber eines KFZs mit einer bestimmten Seriennummer, dann hat er - unter Vorlage der Seriennummer und eines Inhabernachweises - nach der DSGVO Anspruch auf Auskunft aller dieser Schadensdaten. Ein geeigneter Inhabernachweis wäre etwa ein gültiger Zulassungsschein.

Weitere Beispiele für pseudonyme Verarbeitungen sind CRM-Systeme, die statt den Kundennamen die Kundennummer verwenden, klinische Studien die Patientenkennungen statt Namen verwenden oder auch Log-Dateien von Webservern, die IP-Adressen und Gerätekennungen aufzeichnen.

In allen Fällen besteht mit der DSGVO ein Auskunftsanspruch, wenn die Kundennummer, die Patientennummer oder auch die IP-Adressen vorgelegt werden und die Zuordnung zur eigenen Person glaubhaft gemacht wird.

WERDEN SIE MITGLIED DER ARGE DATEN!

ZIELE DER ARGE DATEN

Die ARGE DATEN beschäftigt sich seit 1983 intensiv mit Fragen des Informationsrechts, der Privatsphäre, der Entwicklung des Internets, des Datenschutzes, der Telekommunikation und des Einsatzes neuer Techniken in der Arbeitswelt. Durch Öffentlichkeitsarbeit, Stellungnahmen zu Gesetzesentwürfen, eigenen Gesetzesinitiativen, Publikationen und Seminare konnten in vielen Bereichen der Informationstechnik grundlegende Denkanstöße und Entwicklungen initiiert werden und damit ein verbesserter Betroffenenschutz erreicht werden.

MITGLIEDSCHAFT

Die Mitgliedschaft gilt für ein Kalenderjahr. Sie verlängert sich automatisch um ein weiteres Jahr, wenn sie nicht 3 Monate vor Ablauf der Mitgliedschaft gekündigt wird. Die Generalversammlung der ARGE DATEN hat die Berechtigung den Mitgliedsbeitrag jederzeit zu verändern.

ORDENTLICHES MITGLIED:

Die klassische Mitgliedsform. Ordentliche Mitglieder haben Zugang zum Informationsdienst der ARGE DATEN, werden über laufende Aktivitäten informiert und erhalten kostenlose telefonische Auskünfte zu informationsrechtlichen Fragen aller Art. Durch die Mitgliedschaft vieler Personen kann die ARGE DATEN auch die Anliegen zur Verbesserung des Datenschutzes in Österreich wirksam vertreten.

- Jahresbeitrag Ordentliches Mitglied/Einzelperson: 40,- EUR.
- Jahresbeitrag Ordentliches Mitglied/Familien bzw. Lebenspartner (gemeinsamer Haushalt): 55,- EUR.
- Jahresbeitrag Ordentliches Mitglied/Institution (Vereine, Firmen und sonstige Organisationen):
- Mitgliedschaft SMALL: 90,- EUR
- Mitgliedschaft MEDIUM: 350,- EUR
- Mitgliedschaft LARGE: 700,- EUR

* **SMALL:** kleine Organisationen mit wenigen Mitarbeiter, wenigen Kunden und wenigen Datenverarbeitungen, zB Gewerbebetriebe, EPUs, Freizeitvereine

* **MEDIUM:** KMUs mit mehr als 50 Mitarbeiter oder Interessenvertretungen mit mehr als 100 Mitgliedern oder Organisationen mit Verarbeitungen von Daten besonderer Datenkategorien

* **LARGE:** größere Organisationen mit internationalen Tätigkeiten, vielen Mitarbeitern, vielen Kunden oder vielen Verarbeitungen

Bestehen Unklarheiten in der Zuordnung einer Organisation behält sich der Vorstand die Letztentscheidung vor.

FÖRDERNDES MITGLIED:

Zielpublikum für diese Mitgliedsform sind Personen und Institutionen, die die ARGE DATEN besonders finanzielll unterstützen wollen. Die Höhe des Mitgliedsbeitrages ist grundsätzlich frei gewählt, darf aber nicht unter 100,- EUR liegen. Im Gegensatz zur ordentlichen Mitgliedschaft besteht kein Stimmrecht in der Generalversammlung.

Es wird der ARGE DATEN dadurch möglich, auch in Zukunft konsequent die Entwicklungen der Informationsverarbeitung zu analysieren und Trends darzustellen.

LEISTUNGEN DER ARGE DATEN

a. PRIVACY Unterstützung
b. Zusendung des Informationsdienstes der ARGE DATEN.
c. Rabatte bei Veranstaltungen und Seminaren.
d. Sonderkonditionen bei der Nutzung des ARGE DATEN - Dienstleistungsangebots.
e. Kostenlose Datenschutz-Erstauskunft.

An die ARGE DATEN
Österreichische Gesellschaft für Datenschutz
1160 Wien, Redtenbachergasse 20

ANTRAG AUF MITGLIEDSCHAFT:

Frau/Herr/die Organisation/der Verein/das Unternehmen

_____

Zustelladresse:

_____

Telefon: _____

Telefax: _____

Mail: _____

Der Mitgliedsbeitrag ist ab Datum der Bestätigung der ordentlichen Mitgliedschaft fällig jeweils für das Kalenderjahr.
Informationen gemäß DSGVO
http://www.argedaten.at/dsgvo.html
(auf Wunsch erhalten Sie das Informationsblatt auch zugeschickt)

ART DER MITGLIEDSCHAFT:

a. Ordentliches Mitglied - Einzelperson (40,- EUR) ☐
b. Ordentliches Mitglied - Lebenspartner (55,- EUR) ☐
c. Ordentliches Mitglied - Organisation Gruppe I (SMALL 90,- EUR) ☐
d. Gruppe II (MEDIUM 350,- EUR) ☐
e. Gruppe III (LARGE 700,- EUR) ☐
f. förderndes Mitglied mit dem Förderbeitrag

_____EUR zutreffendes bitte ankreuzen/ausfüllen

Ort, Datum: _____

Rechtsgültige Unterschrift/Stempel:

_____

PRIVACY POLICY

PRIVACY POLICY ist ein Service der ARGE DATEN, das Verantwortliche, Auftragsverarbeiter und Betroffene bei Umsetzung der Rechte und Pflichten gemäß Datenschutzgrundverordnung (DSGVO) unterstützt. Das Service umfasst sowohl Musterschreiben und Checklisten für die eigenständige Umsetzung der Datenschutzanforderungen. Enthält aber auch Beratung, bis hin zur Vertretung und Kostenübernahme in Datenschutzverfahren die für eine größere Zahl von Mitgliedern von Bedeutung sind.
Die Erstberatung ist kostenlos, in vielen Fällen ist sie meist auch ausreichend für die Wahrnehmung der Datenschutzinteressen. Bei komplexen Fragestellungen oder Gutachten muss ein angemessener Kostenbeitrag geleistet werden. Voraussetzung für jede Vertretung ist eine umfassende Dokumentation der Datenschutzverletzung, die Bereitstellung aller relevanten Unterlagen in Kopie sowie die Erteilung der für das Verfahren notwendigen Vollmacht. Grundsätzlich besteht kein Anspruch auf Vertretung, die Entscheidung ob eine Vertretung erfolgt und über eine finanzielle Unterstützung obliegt dem Vorstand im Einzelfall.

AUSZUG AUS DEN VEREINSSTATUTEN:

ZIELE DER ARGE DATEN (§ 2):
(1) Der Verein bezweckt die Erforschung von Wechselwirkungen zwischen EDV-Einsatz, Informationsrecht, Datenschutz und Gesellschaft. Er wird die Öffentlichkeit und die Fachwelt über erkennbare, vorhersehbare und wahrscheinliche Wechselwirkungen dieser Bereiche informieren. Der Verein wird darauf hinwirken, dass Informationstechnik und Telekommunikation menschengerecht, gesellschaftlich verantwortbar und unter Wahrung des Schutzes personenbezogener Daten, sowie unter Wahrung des Rechts auf informationelle Selbstbestimmung eingesetzt und weiterentwickelt werden.

(2) Der Verein ist parteipolitisch unabhängig und seine Tätigkeit ist nicht auf Gewinn gerichtet. Er verfolgt ausschließlich und unmittelbar gemeinnützige Zwecke im Sinne § 35 Abs. 2 BAO überwiegend im Inland.

Mittel zur Erreichung des Vereinszwecks (§ 3):

a. Aufbau einer Fachbibliothek und eines Archivs mit Schwerpunkt Informationstechnik, Telekommunikation, Datenschutz und Neue Technik;
b. Aufbau eines elektronischen Informationsnetzes zur raschen Nutzung und Verbreitung wissenschaftlicher Informationen;
c. Aufbau einer Informationsdatenbank zur Dokumentation der Einhaltung des Datenschutzgesetzes bei EDV-Anwendern;
d. fachliche Unterstützung von Gruppen und Initiativen, die dieselben Zwecke verfolgen;
e. Verbreitung der Erkenntnisse auf Fachtagungen, Se-minaren und in öffentlichen Veranstaltungen;
f. Durchführung, Unterstützung oder Vergabe von Untersuchungen bzw. Forschungsvorhaben sowie Erstellung von Unterlagen und Unterrichtsmaterialien;
g. Zusammenarbeit mit nationalen und internationalen Organisationen, die ähnliche Zwecke verfolgen.

WEITERE ANGABEN ZUR MITGLIEDSCHAFT:

Zusätzliche Angaben, die wir bei Anmeldung von insti-tutionellen Mitgliedern benötigen (falls abweichend von den umseitigen Angaben):

AnsprechpartnerIn für die ARGE DATEN:

_____

Adresse:

_____

Telefon:

_____

Alle Informationssendungen der ARGE DATEN sollen an folgende Adresse erfolgen:

_____

_____

_____

Für Fragen der Rechnungslegung ist zuständig:

_____

Adresse:

_____

KENNEN SIE ALLE UNSERE LEISTUNGEN?

Fordern Sie die aktuellen Prospekte und Broschüren an!

☐ **PRIVACY PLUS**
Das Privacy-Komplettpaket speziell für Verantwortliche gemäß DSGVO, inkl. kostenloser Seminarteilnahme, Datenschutz-Audit und Privacy Policy - Beratung
(http://www.argedaten.at/privacyplus)

☐ **KNOW HOW**
Das Seminarangebot der ARGE DATEN
(http://seminar.argedaten.at)

Weitere Informationen zur Mitgliedschaft
http://www.argedaten.at/mitgliedschaft

LÖSCHUNG VON DATEN BEI RELIGIONS-GEMEINSCHAFTEN

Damit gespeicherte Daten vollständig gelöscht werden, sind folgende Schritte erforderlich:

AUSKUNFTSERSUCHEN GEMÄSS ART 15 DSGVO

Als erster Schritt ist an die betreffende Religionsgemeinschaft (Kirche, usw.) ein Auskunftsersuchen gemäß Art 15 Datenschutz-Grundverordnung (DSGVO) zu richten, damit überhaupt bekannt wird, welche konkreten personenbezogenen Daten von dieser gespeichert werden. Nur wenn man weiß, was gespeichert wird, kann man einen Antrag auf Löschung dieser Daten stellen.

RELIGIONSBEKENNTNIS - BESONDERE KATEGORIE PERSONENBEZOGENER DATEN

Gemäß Art 9 DSGVO bilden die personenbezogenen Daten zum Religionsbekenntnis eine besondere Kategorie im Datenschutzrecht und stehen daher unter einem besonderen Schutz. Die Verarbeitung von personenbezogenen Daten besonderer Kategorien verletzt das Datenschutzrecht nicht, wenn die Verarbeitung unbedingt erforderlich ist und geeignete Maßnahmen zum Schutz der Rechte und Freiheiten der Betroffenen gewährleistet sind und darüber hinaus entweder die Verarbeitung gemäß Art 6 DSGVO zulässig ist oder der Betroffene die Daten offenkundig selbst öffentlich gemacht hat.

ZULÄSSIGKEIT DER VERWENDUNG VON PERSONENBEZOGENEN DATEN

Gemäß Art 5 Abs 1 lit b DSGVO dürfen Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden. Aus diesem Grundsatz der Datenverwendung ergeben sich zwei Ansatzpunkte: Erstens ist eine Person nicht Mitglied einer bestimmten Religionsgemeinschaft, so dürfen deren Daten von dieser Religionsgemeinschaft überhaupt nicht ermittelt werden. Zweitens war die betreffende Person Mitglied dieser Religionsgemeinschaft und ist sie aus dieser ausgetreten, so dürfen die zuvor ermittelten Daten nicht weiterverarbeitet werden und sind von der Religionsgemeinschaft von sich aus zu löschen.

SPEICHERUNG VON DATEN IN PERSONENBEZOGENER FORM

Daten dürfen gemäß Art 5 Abs 1 lit e DSGVO nicht länger in personenbezogener Form gespeichert werden, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Auch aus diesem Grundsatz der Datenverarbeitung ergibt sich, dass die Daten ab dem Zeitpunkt wo sie nicht mehr zur Zweckerfüllung erforderlich sind, nicht mehr in personenbezogener Form, sondern nur noch anonymisiert aufbewahrt werden dürfen.

RECHT AUF LÖSCHUNG PERSONENBEZOGENER DATEN

Jede Religionsgemeinschaft hat gemäß Art 17 Abs 1 DSGVO personenbezogene Daten aus eigenem Antrieb oder auf Antrag der betroffenen Person unverzüglich zu löschen, wenn die Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind oder die personenbezogenen Daten unrechtmäßig verarbeitet wurden oder die Löschung der Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist oder die Einwilligung des Betroffenen widerrufen wurde. Dies bedeutet, dass eine Religionsgemeinschaft alle personenbezogenen Daten eines Betroffenen unverzüglich von sich aus zu löschen hat, sobald ihr bekannt ist, dass die betreffende Person nicht Mitglied ihrer Gemeinschaft ist. Dasselbe gilt für den Fall, dass die Religionsgemeinschaft von sich aus Daten über Personen ermittelt und dabei feststellt, dass diese Person nicht Mitglied ihrer Organisation ist. Daraus ergibt sich wiederum, dass es rechtwidrig ist, dass Religionsgemeinschaften personenbezogene Daten von Personen ermitteln, die nicht Mitglieder bei ihr sind.

ANTRAG AUF LÖSCHUNG PERSONENBEZOGENER DATEN

Wurde durch das Auskunftsersuchen gemäß Art 15 DSGVO festgestellt, dass eine Religionsgemeinschaft personenbezogene Daten über eine Person speichert, die kein Mitglied dieser Organisation ist, so liegt eine unzulässige Datenverarbeitung vor. Bei einer unzulässigen Datenverarbeitung hat die betreffende Person das Recht auf Löschung dieser Daten und kann einen diesbezüglichen Antrag an die Religionsgemeinschaft stellen, mit der Begründung, dass es sich um eine unzulässige Datenverarbeitung handelt, da man nicht Mitglied ist.

LÖSCHUNG INNERHALB EINES MONATS

Wurde ein Löschungsantrag gestellt, so müssen gemäß Art 12 Abs 2 DSGVO die personenbezogenen Daten unverzüglich, in jedem Fall aber innerhalb eines Monats ab Antragstellung, von der Religionsgemeinschaft gelöscht werden und der Antragsteller ist von der Löschung zu verständigen. Wird die Löschung verweigert, so ist der Antragsteller (Betroffene) ebenfalls innerhalb eines Monats schriftlich zu verständigen und es ist zu begründen, warum die Löschung nicht vorgenommen wird.

RECHT AUF EINSCHRÄNKUNG DER VERARBEITUNG GEMÄSS ART 18 DSGVO

Betroffene haben das Recht auf Einschränkung, solange keine Feststellung über die Richtigkeit oder Unrichtigkeit der personenbezogenen Daten besteht. Darüber hinaus sind Einschränkungen zulässig, wenn ein Widerspruchsrecht des Betroffenen eingelegt wurde. Weiters kann ein Betroffener eine Einschränkung seiner Datenverarbeitung verlangen, wenn die Verarbeitung unrechtmäßig ist und keine Löschung verlangt wurde. Schließlich kann der Betroffene eine Einschränkung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen verlangen. In den oben genannten Gründen darf die Religionsgemeinschaft die personenbezogenen Daten grundsätzlich nur noch speichern, aber keine Verarbeitungsschritte durchführen.

Eine Weiterverarbeitung ist nur zulässig, wenn die Einwilligung des Betroffenen vorliegt oder dies zur Ausübung oder Verteidigung von Rechtsansprüchen des Verantwortlichen notwendig ist. Weiters darf die Religionsgemeinschaft eine Datenverarbeitung durchrühren, wenn dies zum Schutz der Rechte einer anderen natürlichen oder juristischen Person erforderlich ist oder es aus Gründen eines wichtigen öffentlichen Interesses notwendig ist.

SANKTIONEN BEI VERWEIGERUNG DER LÖSCHUNG

Wird das Recht auf Löschung der personenbezogenen Daten verletzt, so ist gemäß 83 Abs 5 DSGVO eine Geldstrafe von bis zu 20 Millionen oder im Fall eines Unternehmens von bis zu 4 % des globalen Jahresumsatzes zu zahlen. Hat die Datenschutzverletzung auch einen materiellen oder immateriellen Schaden zur Folge, dann entsteht zusätzlich ein Recht auf Schadenersatzklage des Betroffenen gemäß Art 82 DSGVO. Die Landesverwaltungsgerichte sind für Schadenersatzklagen zuständig.

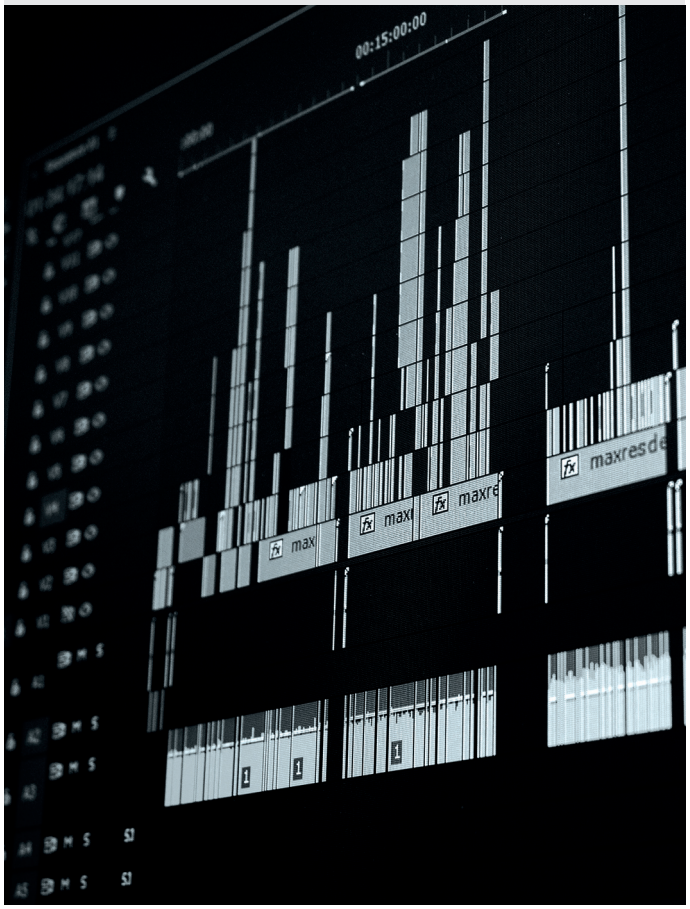
VERWENDUNG VON TONDOKUMENTEN OHNE EINWILLIGUNG VON BETROFFENEN

Die Thematiken "Videoüberwachung" sowie "Recht am eigenen Bild" sind zum regelmäßigen Bestandteil täglicher Berichterstattung geworden. Die Frage, unter welchen Umständen Tondokumente, die Stimmaufnahmen anderer Personen enthalten, angefertigt sowie verwendet werden dürfen, ist dagegen nicht sehr präsent. Dabei handelt es sich auch hier um erhebliche Eingriffe in Persönlichkeitsrechte.

STRAFRECHTLICHE BESTIMMUNGEN

Gegen Verletzungen des Rechts am eigenen Wort kann nicht nur zivil-, sondern auch strafrechtlich vorgegangen werden. Die entsprechende Regelung bildet § 120 Strafgesetzbuch (StGB). § 120 Abs 1 StGB stellt die Verwendung eines Tonaufnahmegerätes oder Abhörgerätes unter Strafe, wenn dies dazu dient, sich von einer nicht öffentlichen und nicht für denjenigen zur Kenntnisnahme bestimmten Äußerung, Kenntnis zu verschaffen. Die Strafdrohung beträgt bis zu einem Jahr Freiheitsstrafe bzw. bis zu 360 Tagessätzen Geldstrafe.

Dabei ist zu beachten, dass § 120 Abs 1 StGB die Vornahme von Tonaufzeichnungen eben nur dann unter Strafe stellt, wenn die entsprechende Äußerung "nicht öffentlich" erfolgt Erfasst wird durch diese Strafbestimmung somit das Abhören von Gesprächen, an denen der Aufzeichnende gar nicht teilnimmt. Das Aufzeichnen von Äußerungen, die direkt an den Tonaufzeichnenden gerichtet sind, ist hingegen nach § 120 Abs 1 StGB nicht strafbar. Gibt der Aufzeichnende allerdings die so erlangten Tonaufnahmen ohne Einwilligung des Betroffenen an einen Dritten weiter, für den diese nicht bestimmt sind, verstößt er gegen §120 Abs 2 StGB.



Kurz zusammengefasst: Gerichtlich strafbar ist es, Tondokumente von Äußerungen herzustellen, die gar nicht an denjenigen gerichtet waren, der die Aufzeichnung vornimmt (klassisches "Abhören" fremder Gespräche). Ebenso gerichtlich strafbar ist die Weitergabe von Tondokumenten an Dritte ohne Einwilligung des Betroffenen. Es unterliegt jedoch nicht dem Strafrecht, wenn aus aufgezeichneten Gesprächen, an denen der Aufzeichnende teilnimmt, Tondokumente produziert werden, die keinem Dritten zugänglich gemacht werden.

§ 120 Abs 2aStGB verfolgt hingegen Verstöße gegen das Übertragungsgeheimnis im Bereich der Telekommunikation und bestraft die Aufzeichnung, Weitergabe und Veröffentlichung von Telekommunikationsnachrichten, welche nicht für denjenigen bestimmt sind, der die Aufzeichnung vornimmt.

Sämtliche Begehungsformen des § 120 StGB sind sogenannte Ermächtigungsdelikte, was bedeutet, dass eine Verfolgung des Täters nur mit Ermächtigung des Tatopfers stattfindet.

RECHTFERTIGUNGSGRÜNDE

Ebenso kompliziert und breit gefächert wie der strafrechtliche Tatbestand, ist auch die Judikatur, wann entsprechende Eingriffe in das Recht am eigenen Wort gerechtfertigt sein können.

Prinzipiell orientiert sich die Rechtsprechung an den allgemeinen strafrechtlichen Rechtfertigungsgründen von Notwehr und Notstand und erlaubt in Einzelfällen eine Verwendung strafrechtswidrig ermittelter Tondokumente auch in Verwaltungs- und Gerichtsverfahren. Als zulässig wurden das Herstellen und die Weitergabe entsprechender Aufnahmen zur Abwehr einer Erpressung beurteilt. Nicht gerechtfertigt sind hingegen die Verwendung illegal erstellter Tonaufnahmen als Beweismittel in einem Scheidungsverfahren.

In Strafprozessen gilt die Verwendung widerrechtlicher Tonmitschnitte als zulässig, wenn dies der Wahrung der Verteidigungsrechte des Beschuldigten dient. Grundsätzlich gibt es allerdings noch keine abschließend klärende Judikatur, in welchen Fällen eine Verwertung von Tondokumenten, trotz rechtswidriger Erstellung in entsprechenden Verfahren, zulässig sein kann. Darüber muss immer im jeweiligen Einzelfall entschieden werden.

Weiteres ist darauf zu verweisen, dass für Tonaufzeichnungen, welche durch Behörden in Ausübung entsprechender Kompetenzen, etwa im Rahmen der StPO, angefertigt werden, natürlich gesonderte Regelungen existieren.

PERSÖNLICHKEITSRECHTE

Über die strafrechtlichen Bestimmungen hinaus stehen Betroffenen zivilrechtliche Unterlassungsansprüche zu. Grundsätzlich greift die Aufzeichnung von Tondokumenten, welche Stimmaufnahmen anderer Personen wiedergeben, in das Persönlichkeitsrecht von Betroffenen, das Recht am eigenen Wort, ein.Eine gesetzliche Regelung, auf die entsprechende Persönlichkeitsrechte gestützt werden können, ist § 16 ABGB, der den Schutz der Privatsphäre festlegt.

Auf Grundlage dieser Bestimmung wurden die Tonbandaufnahmen einer geschäftlichen Besprechung unter vier Augen, ohne Zustimmung des Gesprächspartners, oder die heimliche Aufnahme eines Gespräches mit dem Arbeitgeber durch einen Angestellten, als rechtswidrig beurteilt. (3 Ob 131/00m, 6 Ob 190/01m)

Weiter ist darauf hinzuweisen, dass die Aufzeichnung von Gesprächsäußerungen anderer Personen auch urheberrechtliche Konsequenzen haben kann. Dies ist bei Äußerungen urheberrechtlichen "Werkcharakters" der Fall, vor allem bei öffentlichen Reden oder Vorträgen. Eine Aufzeichnung auf Tonträgern und Verbreitung von solchen Äußerungen ist nach § 43 UrhG nur mit Einwilligung des Urhebers möglich bzw. dann, wenn dieser seine Werknutzungsrechte an den Aufzeichnenden abtritt.

SIND TONDOKUMENTE PERSONENBEZOGENE DATEN?

Die Frage in wie weit das Datenschutzgesetz auf Tondokumente, welche persönliche Äußerungen wiedergeben, anwendbar ist, rückt aufgrund der umfangreichen Regelung im StGB in den Hintergrund.

Grundsätzlich ist davon auszugehen, dass derartige Mittschnitte, sofern sie auf eine bestimmte Person rückführbar sind, jedenfalls personenbezogene Daten darstellen, da auch ein "bestimmbarer" und nicht nur unmittelbar bestimmter Personenbezug ausreicht, um Daten dem Anwendungsbereich des Datenschutzgesetzes zu unterstellen. Mit der Entscheidung K503.425-090 /0003-DVR/2005 hat auch die Datenschutzbehörde bestätigt, dass grundsätzlich Tondokumente - unter der Bedingung eines bestimmbaren Personenbezugs- dem Datenschutzgesetz unterliegen. Das bedeutet, dass entsprechende Ansprüche wegen widerrechtlicher Verwendung von personenbezogenen Tonaufnahmen ergänzend zum StGB sowie zu allgemeinen, zivilrechtlichen Ansprüchen auch auf das Datenschutzgesetz gestützt werden können. Da die Herstellung personenbezogener Tonaufnahmen ohne Einwilligung des Betroffenen nur in beschränktem Ausmaß dem § 120 StGB unterliegt, kann hier ergänzend das Datenschutzgesetz herangezogen werden, um sich gegen solche Tonaufnahmen zu wehren.

Je nach Inhalt des entsprechenden Tondokuments kann es sich auch um personenbezogene Daten besonderer Kategorien handeln und ist, wie auch bei anderen Eingriffen in das Grundrecht auf Datenschutz, je nach Anlassfall eine Abwägung, zwischen den Interessen des Aufzeichnenden und den Rechten des Betroffenen, durchzuführen.

RESÜMEE

Bezüglich Herstellung und Verwendung personenbezogener Tondokumente gibt es in Österreich umfassende Regelungen, die sich allerdings im Überschneidungsbereich zwischen allgemeinem Zivilrecht, gerichtlichem Strafrecht, Urheberrecht und Datenschutz bewegen. In diesem Zusammenhang ist zu überlegen, ob die Vornahme von Tonaufzeichnungen im Zusammenhang mit Videoüberwachungsmaßnahme durch Private nicht sogar strafrechtlich relevant sein kann. Generelle Präventivmotive können jedenfalls kein Rechtfertigungsgrund sein, der die Herstellung personenbezogener Tondokumente durch Private, ohne Einwilligung von Betroffenen, rechtfertigt.

DATENSCHUTZSTENOGRAMM 2017/18

- **17. Jänner 2018 DSB (DSB-D213.503/0004-DSB/2017): Verbot des Zugriffs von AMS-Trainern auf Daten von Kursteilnehmern**
- **13. Dezember 2017 DSB (DSB-D213.531/0009-DSB/2017): Verbot der zeitlich unbefristeten Speicherung von Protokolldaten**
- **12. Dezember 2017 VwGH (E3249/2016): Recht auf Datenlöschung und Vernichtung sämtlicher bei einem Finanzamt aufbewahrter Papierakten**
- **20. Dezember 2017 EuGH (C-434/16): Umfang der Rechte der betroffenen Person auf Auskunft und auf Berichtigung**
- **22. November 2017 DSB (DSB-D216.309/0007-DSB/2017): Verbot der Privat-Sheriff-Tätigkeit mittels Videoüberwachung**
- **27. September 2017 EuGH (C-73/16): Erstellung einer Liste mit personenbezogenen Daten zum Zweck Steuererhebung, Bekämpfung von Steuerbetrug**
- **5. September 2017 EGMR (61496/08): Überwachung der Internetnutzung durch Arbeitgeber unzulässig**
- **28. Juni 2017 DSB (DSB-D213.541/0005-DSB/2017): Verbot der Verwendung der Sozialversicherungsnummer außerhalb von Sozialversicherungszwecken**
- **1. Juni 2017 DSB (DSB-D213.547/0005-DSB/2017): Verbot Gewerbedaten an Wirtschaftskammer zur „Pfuscherbekämpfung“ zu übermitteln**
- **4. Mai 2017 EuGH (C-13/16): Erforderlichkeit zur Verwirklichung des berechtigten Interesses eines Dritten**
- **21. März 2017 DSB (DSB-D215.937/0003-DSB/2017): Verbot Telefonnummern ohne Zustimmung zu Wahlwerbe-SMS zu verwenden**
- **15. März 2017 EuGH (C-536/15): Zurverfügungstellung personenbezogener Teilnehmerdaten zum Zweck der Bereitstellung von öffentlich zugänglichen Auskunftsdiensten und Teilnehmerverzeichnissen**
- **9. März 2017 EuGH (C-398/15): Offenlegung im Gesellschaftsregister unterliegende Daten**
- **2. März 2017 DSB (DSB-D213.453/0003-DSB/2016): Verbot öffentliche Bereiche mit Video zu überwachen**
- **26. Jänner 2017 DSB (DSB-D213.468/0001-DSB/2017): Empfehlung ausreichende Datenschutzmaßnahmen in Krankenhaus umzusetzen (erging an zahlreiche Krankenanstalten)**
- **18. Jänner 2017 VwGH (Ra 2016/18/0197): Datenschutz ist auch im Zusammenhang von Asylverfahren zu beachten**

PRIVATSPHÄRE - DER LANGE WEG VON DER IDEE ZUR UMSETZUNG

1890 schrieben die beiden US-Topjuristen Warren und Brandeis in der Harvard Law Review erstmals zum Thema Privatsphäre („The Right to Privacy"). Dieser Artikel gilt als Geburtsstunde des Rechts auf Privatsphäre. Entstanden war damals die Idee der Privatsphäre auf Grund einer technologischen Neuerung, der Kleinbildkamera. Sie erlaubte es erstmals relativ unbemerkt Bilder von Personen - auch gegen deren Willen - anzufertigen. Aus dem „right to be let alone", aus dem Recht allein gelassne zu werden, sollte laut EU - wieder als Reflex auf eine technische Neuerung - ein „right to be forgotten" werden, ein Recht auf Vergessen in den unübersehbaren Abgründen des Internets.

DATENSCHUTZ-MEILENSTEINE

Viel ist seit 1890 in Sachen Datenschutz passiert, vieles ist aber auch noch offen, hier eine kurze Geschichte zum Datenschutzgesetz.

18. OKTOBER 1978: Erstes österreichisches Datenschutzgesetz wird beschlossen
1. JÄNNER 1980: Erstes österreichisches Datenschutzgesetz tritt in Kraft
1983: deutsches Bundesverfassungsgericht formuliert im Volkszählungsurteil „informationelles Selbstbestimmungsrecht"
24. OKTOBER 1995: EG-Datenschutzrichtlinie 95/46/EG tritt in Kraft
1. JÄNNER 2000: Datenschutzgesetz 2000 (DSG 2000) tritt in Kraft
1. JULI 2000: Standard- und Muster-Verordnung 2000 (StMV) tritt in Kraft
18. MAI 2001: Deutschland veröffentlicht neues Datenschutzgesetz
12. JULI 2002: EG-RICHTLINIE 2002/58/EG Datenschutzrichtlinie für elektronische Kommunikation tritt in Kraft
27. JULI 2004: Verabschiedung der Standard- und Muster-Verordnung 2004 StMV 2004
2008: deutsches Bundesverfassungsgericht formuliert im Online-Durchsuchungsurteil das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"
1. JÄNNER 2010: DSG-Novelle 2010 regelt erstmals Videoüberwachung
25. JÄNNER 2012: Die Europäische Kommission stellt Entwürfe zur Überarbeitung des Europäischen Datenschutzrechts vor
26. OKTOBER 2012: Die EU-Grundrechtecharta, in der in Art. 8 Datenschutz ausdrücklich als Grundrecht verankert wird, wird im Amtsblatt veröffentlicht
APRIL 2013: Insgesamt werden mehr als 3.000 Änderungsvorschläge an der DSGVO von Europaparlamentariern eingebracht
1. MAI 2013: DSG-Novelle 2013 - Reaktion auf das Urteil des Europäischen Gerichtshofs wird die Datenschutzkommission durch die Datenschutzbehörde ersetzt
20. JULI 2013: Inkrafttreten der österreichischen Datenschutzanpassungs-Verordnung 2013
31. DEZEMBER 2013: Inkrafttreten einer Änderung der österreichischen Standard- und Muster-Verordnung 2004
12. MÄRZ 2014: Das Europäische Parlament bestätigt mit großer Mehrheit das im LIBE-Ausschuss (Oktober 2013) beschlossene Verhandlungsmandat zur neuen EU-Grundverordnung Datenschutz (621 JA-Stimmen, 10 NEIN-Stimmen und 22 Enthaltungen
28. JÄNNER 2016: Pünktlich zum Europäischen Datenschutztag veröffentlichen EU-Rat und Parlament die politische Einigung zur DSGVO
4. MAI 2016: Die Datenschutz-Grundverordnung (DSGVO) wird im Amtsblatt der Europäischen Union veröffentlicht und muss mit einer Übergangsfrist von zwei Jahren in allen Mitgliedsstaaten angewandt werden
31. JULI 2017: Das neue Datenschutz-Anpassungsgesetz 2018 wird im RIS verlautbart, es tritt zeitgleich mit der DSGVO am 25. Mai 2018 in Kraft
13. OKTOBER 2017: Art. 29 - EU-Datenschutzgruppe veröffentlicht Leitlinien zur Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA)
20. APRIL 2018: Nationalrat beschließt ein „Datenschutz-Deregulierungsgesetz" mit zahllosen Einschränkungen der DSGVO und Abschwächungen des noch nicht einmal in Kraft befindlichen Datenschutz-Anpassungsgesetz 2018
16. MAI 2018: Das Datenschutz-Anpassungsgesetz 2018 - Wissenschaft und Forschung - WFDSAG 2018 ändern Datenschutzbestimmungen in 17 Gesetzen
17. MAI 2018: Das erste Datenschutzanpassungspaket wird im Bundesgesetzblatt veröffentlicht. 125 Gesetze sind betroffen
25. MAI 2018: Ab diesem Tag MUSS die Datenschutz-Grundverordnung in allen EU-Mitgliedstaaten unmittelbar angewendet werden. In Österreich gilt zusätzlich das neue DSG

Worauf hat die DSGVO keine Antworten?
Die Liste ist lang und wird angesichts der technologischen Entwicklungen immer länger:

- **INTERNET-OF-THINGS:** die Vernetzung heterogener Systeme wirft völlig neue Fragen zur Datenqualität, Verantwortlichkeit für den Gesamtprozess und Durchschaubarkeit für die Benutzer auf
- **DIGITALE ASSISTENZ:** völlig ungeklärt ist die Absicherung der Privatsphäre gegenüber den Operatoren, die fernab, aus völlig anderen Kultur- und Gesellschaftskreisen kommen und intime Einblicke in das Leben der Nutzer erhalten
- **DATENABSTRAKTION:** wenn aus personenbezogenen Daten nicht anonyme Daten werden, wer Garantiert die Anonymität, wer garantiert, dass keine Rückwirkungen auf individuelle Entscheidungen erfolgen
- **BIG-DATA:** das Schürfen in großen Datenmengen hat vergleichbare Probleme wie die Suche nach Gold. Bestenfalls 0,01 Promille sind werthaltig, der Rest ist taubes Gestein. Wer sichert die Qualität der Datenanalysen? Wer sorgt für die Entsorgung des „tauben Gesteins", sprich des Datenschrotts?
- **INFORMATIONSFREIHEIT:** Der ungefilterte Zugang zu Information ist ein Grundrecht, selbst die Zugangskriterien festzulegen ist notwendige Voraussetzung zur Sicherung der Privatsphäre
- **AUTONOME SYSTEME:** Bisher agierten Systeme nur in geschlossenen Bereichen (Werkhallen, Eisenbahnanlagen, Fahrstühle, ...). Mit dem Eindringen in bisher offene Systeme die nicht abschließend geregelt sind, wie öffentlicher Raum, öffentliche Verkehrsflächen, Umwelt im weitesten Sinn, ergeben sich völlig neue Fragen zum Verhältnis menschliches Verhalten versus programmiertes Verhalten. Am Ende wird wohl die (gesellschaftspolitische) Entscheidung stehen müssen, welches der Verhaltensvarianten Vorrang

EXTERNER DATENSCHUTZ-BEAUFTRAGTER GEMÄß DSGVO

Vorteile eines externen Datenschutzbeauftragten
Seit 25. Mai 2018 müssen zahlreiche Einrichtungen (Verein, Unternehmen, öffentliche Stellen) verpflichtend einen Datenschutzbeauftragten ernennen.

Die Aufgaben des Datenschutzbeauftragten sind vielfältig und umfangreich, sie erfordern sowohl fundierte technische, organisatorische und rechtliche Kenntnisse zum aktuellen Stand in der Informationsverarbeitung.

Besonders für viele kleine und mittlere Einrichtungen eine Herausforderung, der sie sich nicht gewachsen fühlen.

Die ARGE DATEN bietet gemeinsam mit der e-commerce monitoring gmbh die Funktion des „externen Datenschutzbeauftragten" als fundierte Dienstleistung an. Die inhaltlichen Konzepte kommen von der ARGE DATEN, die professionelle Administration von der e-commerce monitoring gmbh.

DREI UNTERSCHIEDLICHE BASISPAKETE
Informationsverarbeiter sind höchst unterschiedlich aufgestellt, wir haben daher drei unterschiedliche Basispakete entwickelt. Ab 400,- Euro monatlich können Sie alle Anforderungen des Datenschutzbeauftragten gemäß DSGVO und DSG (neu) erfüllen.

EXTERNER DATENSCHUTZBEAUFTRAGTER - BASIC

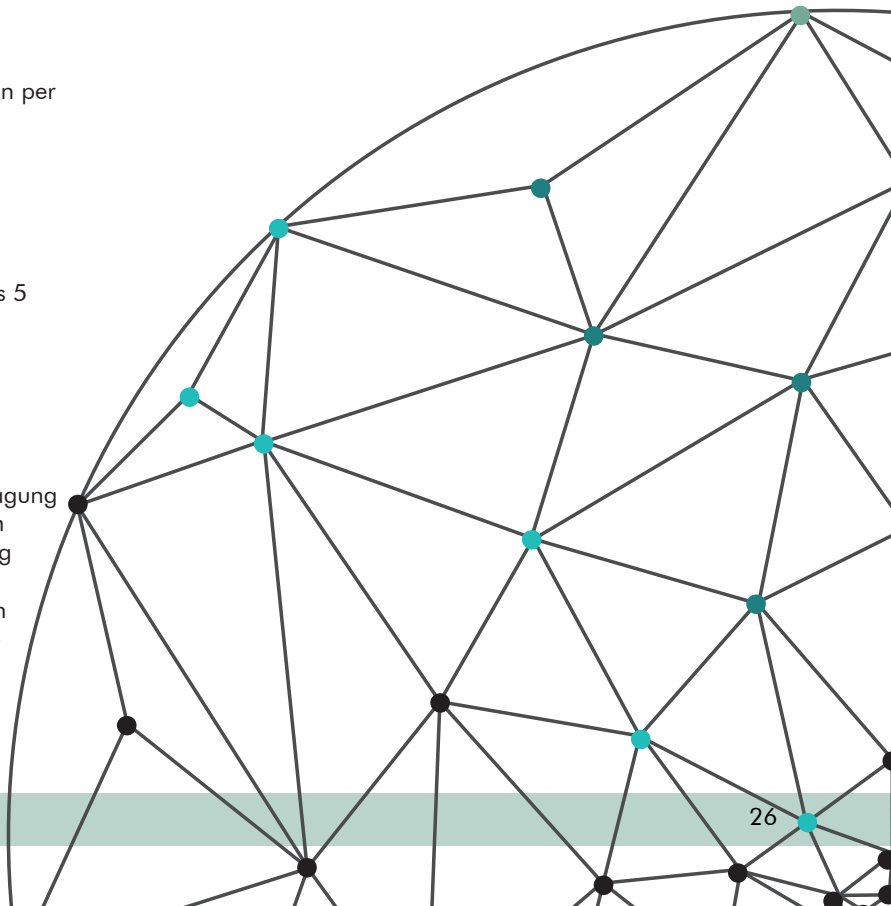
Geeignet für kleine und mittlere Unternehmen mit geringer Zahl an personenbezogenen Datensätzen und geringe Zahl von Verarbeitungen (max 3)

inkludierte Leistungen:
- Ansprechstelle für die Datenschutzbehörde
- laufende Information der Verantwortlichen (Geschäftsführung) zu gesetzlichen und sonstigen wesentlichen Änderungen der Datenschutzbestimmungen per eMail
- jährliches Review der Datenschutzsituation beim Verantwortlichen vor Ort (Ausmaß bis 3 Stunden)
- jährlich ein Datenschutz-Schulungstermin für neue Mitarbeiter (bis 3 Stunden)
- Beantwortung individueller Datenschutzfragen des Verantwortlichen, seiner Mitarbeiter oder Betroffener (bis 5 Fälle/Jahr in Pauschale inkludiert)
- Unterstützung bei datenschutzrelevanten Vorfällen (Auskunftsbegehren, sonstige Begehren Betroffener, Meldeverpflichtungen an die Datenschutzbehörde, etwa im Zusammenhang mit Datenschutzverletzungen (bis 5 Anfragen/Jahr in Pauschale inkludiert)
- kostenlose Teilnahme eines Mitarbeiters bei der Jahrestagung „betrieblicher Datenschutz" (sollte diese Veranstaltung in einem Jahr entfallen, kann eine alternative Veranstaltung gewählt werden)
- Sonderkonditionen für Teilnahme weiterer Mitarbeiter an Veranstaltungen (+10% Rabatt, anrechenbar an andere Rabatte, nicht jedoch bei Sonderaktionen)

EXTERNER DATENSCHUTZBEAUFTRAGTER - MEDIUM

Geeignet für mittlere Unternehmen mit erheblicher Zahl an personenbezogenen Datensätzen und mittlere Zahl von Verarbeitungen (max 10)

inkludierte Leistungen:
- Ansprechstelle für die Datenschutzbehörde
- laufende Information der Verantwortlichen (Geschäftsführung) zu gesetzlichen und sonstigen wesentlichen Änderungen der Datenschutzbestimmungen per eMail
- jährliches Review der Datenschutzsituation beim Verantwortlichen vor Ort (Ausmaß bis 3 Stunden)
- jährliches Review der bestehenden Verzeichnisse der Verarbeitungstätigkeiten (Art 30), der Datenschutzfolgenabschätzung (Art 35), der Auftragsverarbeitungsverträge (Art 28) und der Informationsunterlagen für Betroffene (Art 13,14) in Form der Bereitstellung eines standardisierten Fragebogens zum internen Datenschutz- oder Datensicherheits-Assassments (Ausmaß bis 16 Stunden)
- jährlich ein Datenschutz-Schulungstermin für neue Mitarbeiter (bis 3 Stunden)
- Beantwortung individueller Datenschutzfragen des Verantwortlichen, seiner Mitarbeiter oder Betroffener (bis 10 Anfragen/Jahr in Pauschale inkludiert)
- Unterstützung bei datenschutzrelevanten Vorfällen (Auskunftsbegehren, sonstige Begehren Betroffener, Meldeverpflichtungen an die Datenschutzbehörde, etwa im Zusammenhang mit Datenschutzverletzungen (bis 10 Fälle/Jahr in Pauschale inkludiert)
- Stellungnahme bei Datenschutzfolgenabschätzung (max eine Folgenabschätzung jährlich)
- kostenlose Teilnahme von maximal zwei Mitarbeitern bei der Jahrestagung „betrieblicher Datenschutz" (sollte diese Veranstaltung in einem Jahr entfallen, kann eine alternative Veranstaltung gewählt werden)
- Sonderkonditionen für Teilnahme weiterer Mitarbeiter an Veranstaltungen (+10% Rabatt, anrechenbar an andere Rabatte, nicht jedoch bei Sonderaktionen)

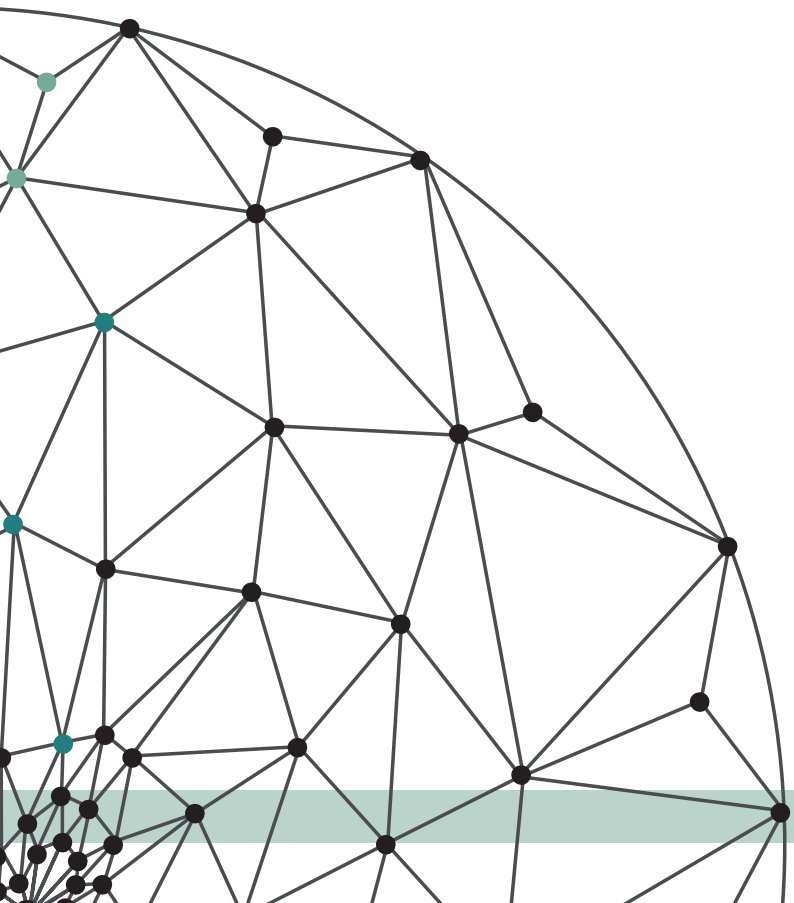


EXTERNER DATENSCHUTZBEAUFTRAGTER - FULL

inkludierte Leistungen:

- Ansprechstelle für die Datenschutzbehörde
- laufende Information der Verantwortlichen (Geschäftsführung) zu gesetzlichen und sonstigen wesentlichen Änderungen der Datenschutzbestimmungen per eMail
- jährliches Review der Datenschutzsituation beim Verantwortlichen vor Ort inklusive Überprüfung von getroffenen Maßnahmen vor Ort (Vor-Ort-Audit) (Ausmaß 2 Manntage)
- jährliches Review der bestehenden Verzeichnisse der Verarbeitungstätigkeiten (Art 30), der Datenschutzfolgenabschätzung (Art 35), der Auftragsverarbeitungsverträge (Art 28), der Informationsunterlagen für Betroffene (Art 13,14) und des Sicherheitskonzepts (Art 32) auf Basis eines mit dem Verantwortlichen abgestimmten Reviewkonzepts (Ausmaß bis 32 Stunden)
- jährlich ein Datenschutz-Schulungstermin für neue Mitarbeiter (bis 3 Stunden)
- Beantwortung individueller Datenschutzfragen des Verantwortlichen, seiner Mitarbeiter oder Betroffener (bis 20 Anfragen/Jahr in Pauschale inkludiert)
- Unterstützung bei datenschutzrelevanten Vorfällen (Auskunftsbegehren, sonstige Begehren Betroffener, Meldeverpflichtungen an die Datenschutzbehörde, etwa im Zusammenhang mit Datenschutzverletzungen (bis 20 Fälle/ Jahr in Pauschale inkludiert)
- kostenlose Teilnahme von maximal drei Mitarbeitern bei der Jahrestagung „betrieblicher Datenschutz“ (sollte diese Veranstaltung in einem Jahr entfallen, kann eine alternative Veranstaltung gewählt werden)
- Sonderkonditionen für Teilnahme weiterer Mitarbeiter an Veranstaltungen (+10% Rabatt, anrechenbar an andere Rabatte, nicht jedoch bei Sonderaktionen)

Indivduelles Angebot
Bei Interesse schicken wir Ihnen gerne ein individuelles Angebot zu: info@e-monitoring.at



OFFENLEGUNG/IMPRESSUM - ARGE DATEN - ÖSTERREICHISCHE GESELLSCHAFT FÜR DATENSCHUTZ

ARGE DATEN - Österreichische Gesellschaft für Datenschutz
A-1160 Wien, Redtenbachergasse 20
UID: ATU56627966

Für Rückfragen, Auskunft und Kontakt wenden Sie sich bitte an:
fon +43(0)1/5320944
fax +43(0)1/5320974
mail info@argedaten.at

registrierter Verein, Vereinsbehörde:
Bundespolizeidirektion Wien ZVR 774004629
http://zvr.bmi.gv.at/Start

Tätigkeit und grundlegende Richtung gemäß Statuten:
http://ftp.freenet.at/legal/statuten.pdf

Vertretung durch den Vorstand, Mitglieder des Vorstandes:
http://www.argedaten.at/php/cms_monitor.php?q=PUB&s=32733tvo

registrierter Zertifizierungsdienste-Anbieter:
http://www.signatur.rtr.at/de/providers/providers/argedaten.html
A-CERT und GLOBALTRUST sind die Markenbezeichnungen der Zertifizierungs- und Signaturdienste gem. SigG / VDG

Information gemäß DSGVO (ab 25.5.2018):
Zweck der Datenverarbeitung gemäß Statuten:
http://ftp.freenet.at/legal/statuten.pdf

Aufsichtstelle iS der DSGVO:
Österreichische Datenschutzbehörde
http://www.dsb.gv.at

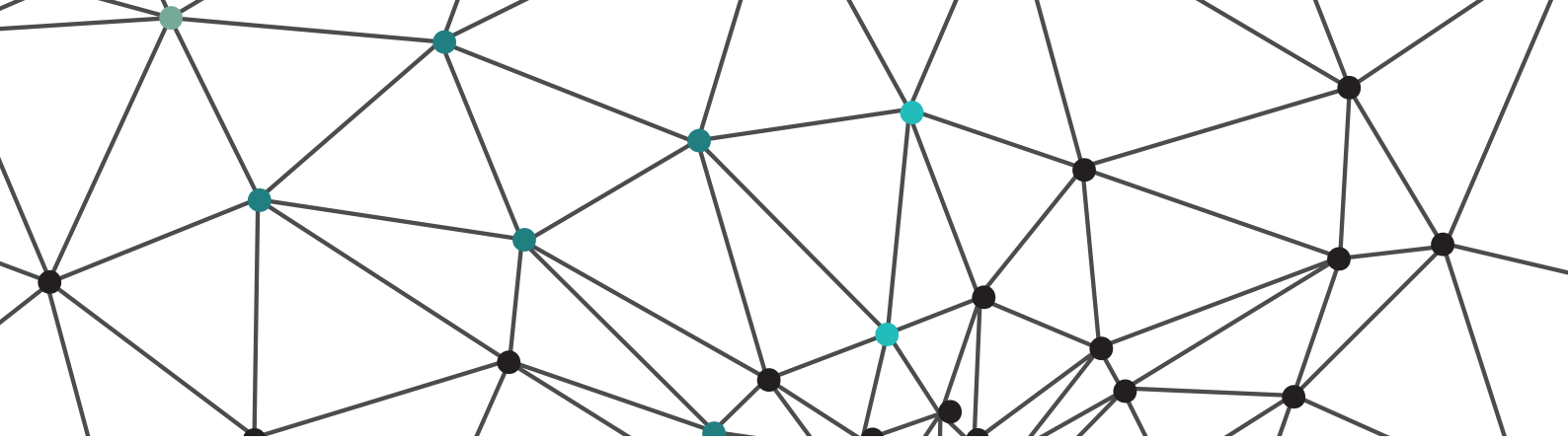
Servicebetrieb zur Abwicklung von Bestellungen und Verrechnung:
e-commerce monitoring GmbH, HG Wien FN 224536 a
http://www.e-monitoring.at

Bildernachweis:
Seite 8,10,15,18 siehe Quelle www.hippopx.com
Seite 23 siehe Quelle www.pexels.com

Mission Statement:
ARGE DATEN ist Österreichs führende Privacy Organisation. Sie setzt sich für den Schutz der Privatsphäre im Zeitalter globaler Informations- und Wirtschaftsprozesse ein.

Tätigkeitsschwerpunkte: Mitgliederbetreuung, Öffentlichkeitsarbeit, Informationsdienst, Gesetzesbegutachtungen und Schulungen. Der Verein arbeitet in enger Kooperation mit Forschungseinrichtungen, Universitäten, der Industrie und Behörden.

ARGE DATEN Privacy Austria wurde 1983 als Arbeitsgruppe gegründet und 1991 als Verein nach österreichischem Recht registriert. Der Verein ist gemeinnützig und parteipolitisch unabhängig. Die ca. 700 Mitglieder sind großteils Unternehmen und andere Organisationen wie Behörden, Universitäten und NGOs.



INHOUSE-SCHULUNG DATENSCHUTZ GEMÄSS DSGVO

Seit 25. Mai 2018 gilt die EU-Grundverordnung Datenschutz (DSGVO) - damit wird Datenschutz erstmals in allen 28 EU-Mitgliedstaaten einheitlich geregelt - das österreichische Datenschutz-Anpassungsgesetz 2018 zur Umsetzung der DSG-VO wurde beschlossen - genau die richtige Zeit sich umfassend zu informieren - http://seminar.e-monitoring.at/inhouse

Für alle EU-Mitgliedstaaten werden einheitliche Regelungen angewendet. Eine einzige Datenschutzbehörde (DPA) ist für eine Organisation verantwortlich abhängig vom Hauptsitz dieser Organisation. Ein europäischer Datenschutzboard wird die DPAs koordinieren.

Für alle Behörden, öffentlichen Stellen und Unternehmen, deren Haupttätigkeit in der „umfangreichen regelmäßigen und systematischen Überwachung von betroffenen Personen" oder in der „umfangreichen Verarbeitung von sensiblen oder strafrechtlich relevanten Daten" besteht, ist ein unabhängiger Datenschutzbeauftragter (DSB) zwingend vorgesehen. So soll die Einhaltung der neuen Regelungen innerhalb der 28 Mitgliedstaaten gewährleistet sein. Unternehmen sind gefordert, sich laufend mit neuen Entwicklungen auseinander zu setzen und rasch darauf zu reagieren.

ARGE DATEN SETZT SCHULUNGSINITIATIVE

In Ihrer InHouse-Schulung geben wir einen Überblick über die geplanten Neuerungen - auf nationaler und auf EU-Ebene. Wir unterstützen Sie bei der Anpassung Ihrer individuellen Datenschutzstrategien angesichts der neuen Entwicklungen.

Fundierte Datenschutz-Schulung scheitert oft am Zeitmangel und dem betrieblichen Alltag. Es ist zu aufwändig wichtige Mitarbeiter auf Schulung zu schicken. Wir haben darauf reagiert, der Datenschutz kommt zu Ihnen. Ihr Vorteil: geringere Reisekosten, fixe Vortragskosten, unabhängig von der Teilnehmerzahl, weniger Zeitaufwand.

Die ARGE DATEN, Österreichs führende Privacy-Organisation, bringt komplexe Datenschutzfragen schnell auf den Punkt. Um unsere Erfahrung möglichst vielen Interessenten weiterzugeben, haben wir ein Ausbildungskonzept entwickelt, das die wachsenden Datenschutz-Anforderungen des Informationszeitalters optimal erfüllt. Das Modul bietet allen Mitarbeitern einen ersten Einstieg in die Datenschutzmaterie. Ideal auch als Einführungsschulung für neue Mitarbeiter.

Liste möglicher Themenschwerpunkte:

- Datenschutzfolgeabschätzung
- Verarbeitungsverzeichnis
- Internationaler Datenverkehr
- Betriebsvereinbarung und Datenschutz
- Videoüberwachung
- Marketing und Remarketing
- Mitarbeiter- und Bewerberdaten
- Entschädigungsansprüche von Betroffenen
- Internet/eMail und Datenschutz
- Datensicherheit
- Whistleblowing
- Telekommunikation und Datenschutz
- Gesundheitsdaten
- Privacy by Design / Privacy by Default
- Überblick ohne spezifische Schwerpunkte

ORGANISATION EINES VERANSTALTUNGSORTS

Wir organisieren auch einen Veranstaltungsort in Ihrer Nähe. Wir verrechnen dazu eine Pauschale von 800,- Euro + den tatsächlichen Veranstaltungskosten (Seminarräume, Verpflegung, Garagenplätze, ...).

Die Teilnehmerzahl ist nicht limitiert, wir empfehlen eine Größe zwischen 8 und 40 Teilnehmern.

REISEAUFWAND

Der Reiseaufwand richtet sich nach der Entfernung zum Auftraggeber, er wird individuell kalkuliert und liegt zwischen EUR 400,- (EUR 480,- inkl. USt) und EUR 800,- (EUR 960,- inkl. USt). Innerhalb Wiens wird pauschaliert EUR 100,- (EUR 120,- inkl. USt) verrechnet.

Die Seminarkosten verstehen sich ohne Kopier-, Raum- und Bewirtungskosten. Der Seminarinhalt wird vorab elektronisch bereitgestellt und kann innerbetrieblich vervielfältigt werden. Auf Wunsch stellen wir auch fertige Seminarmappen zur Verfügung (15,- Euro/Teilnehmer).

Bei Rückfragen sind Ihnen Frau Indra oder Frau Hasil gern behilflich (+43 1 5320944 oder e-Mail info@argedaten.at). Sie erhalten ein unverbindliches Angebot.

HINWEIS! Die Veranstaltung wird von der e-commerce monitoring gmbh, 1110 Wien, Guglgasse 15/3B/6 (HG Wien FN 224536 a) organisiert und abgerechnet. Die inhaltliche Verantwortung liegt bei der ARGE DATEN - Österreichische Gesellschaft für Datenschutz (ZVR 774004629). Alle Preise exkl. USt.