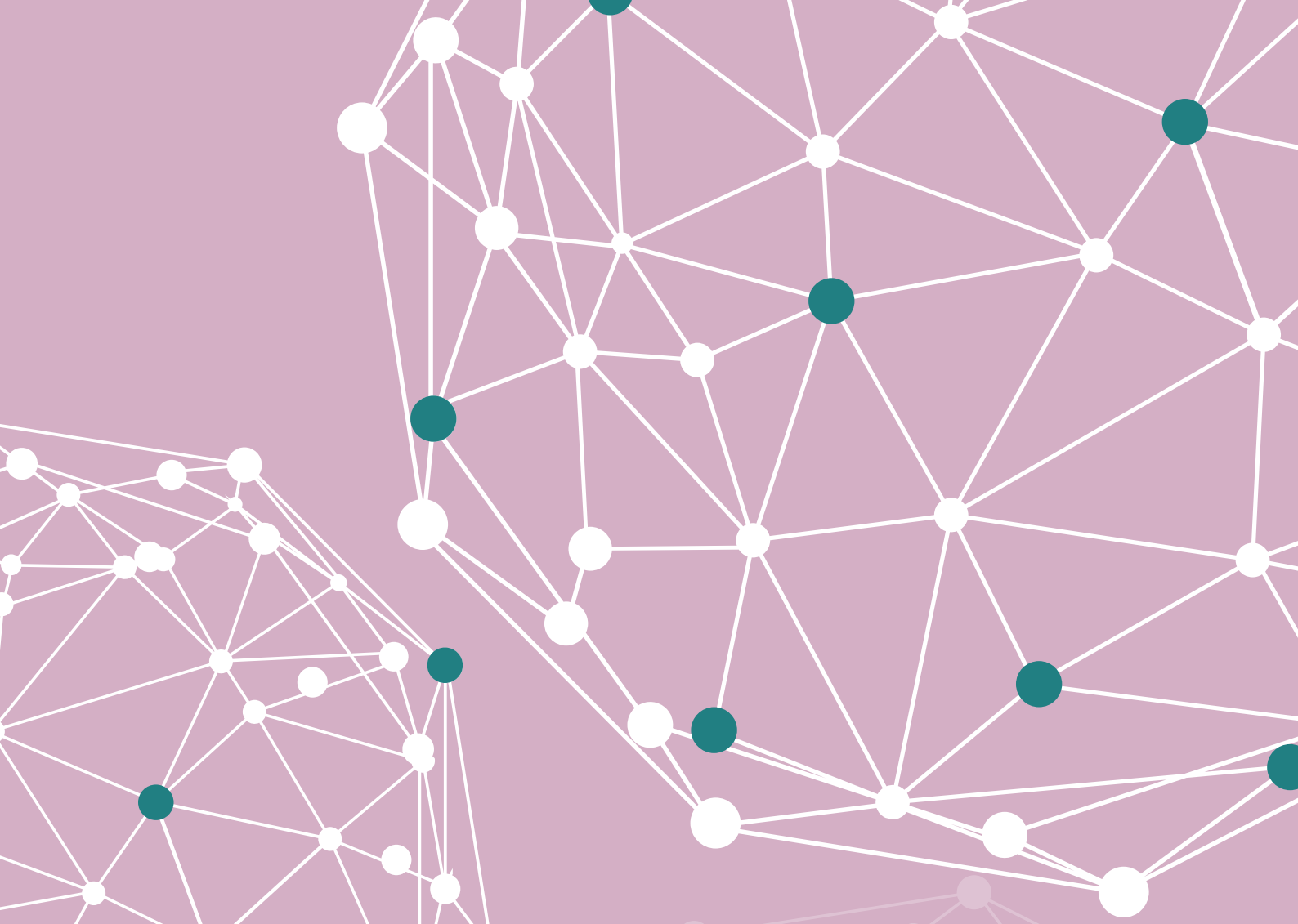
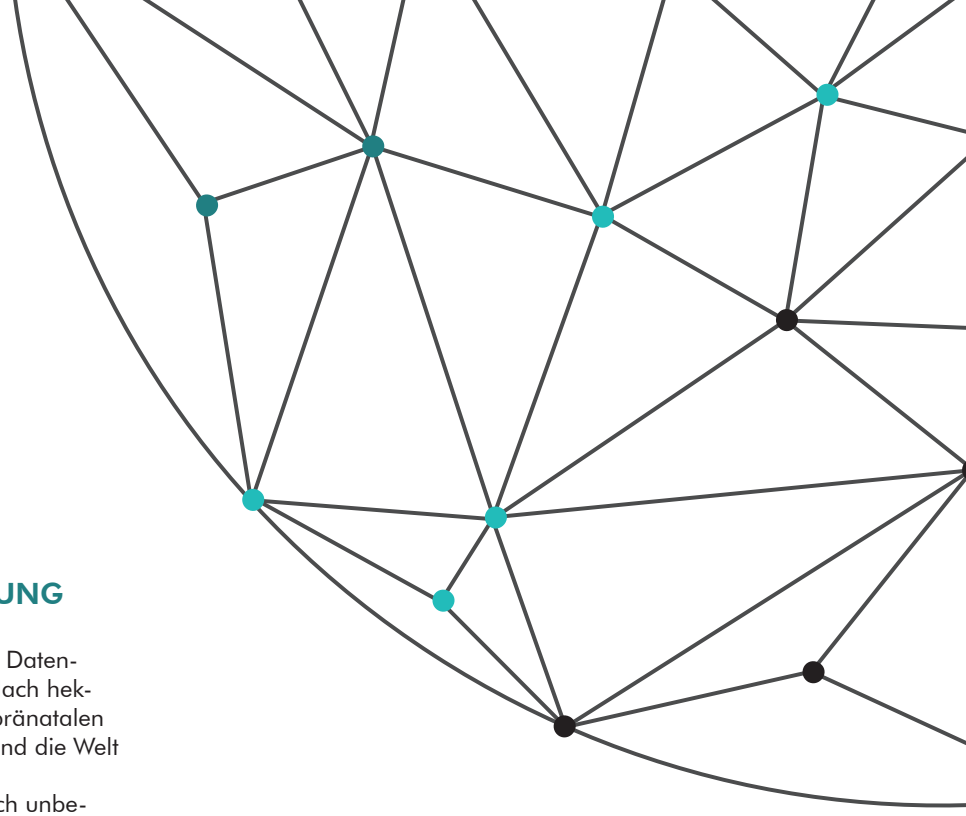


PRIVACY AUSTRIA TÄTIGKEITSBERICHT 2018/19

ARGE DATEN

http://www.argedaten.at/



EDITORIAL

DIE DATENSCHUTZ-GRUNDVERORDNUNG WIRD EIN JAHR ALT

Auf ein turbulentes erstes Jahr kann die europäische Datenschutz-Grundverordnung (DSGVO) zurückblicken. Nach hektischen Vorbereitungen, politischen Turbulenzen im pränatalen Stadium, startete am 25. Mai 2018 die DSGVO ... und die Welt blieb bestehen.

Die großen US-Internetkonzerne blieben offensichtlich unbeeindruckt. Legendär die Antwort des Facebook-Zampanos Marc Zuckerbergs vor dem US-Kongress. „Werden Sie angesichts der letzten Datenskandale [vulgo Cambridge Analytica] Ihr Geschäftsmodell ändern?" Nein, lautete die erwartbare und durchaus ehrliche Antwort.

„Werden Sie angesichts der Datenschutz-Grundverordnung Ihr Geschäftsmodell ändern?" Diese Frage verabsäumte das Europäische Parlament denselben Marc Zuckerberg wenig später zu fragen. Nein, wäre wohl auch hier seine Antwort gewesen.

SCHWERE GEBURT

Der Reihe nach. Natürlich ist das Ein-Jahres-Baby kein Ein-Jahres-Baby. Es hat immerhin 6 Jahre Planung hinter sich, von natürlicher Zeugung, Seitensprung bis In-Vito-Fertilisierung ließ die Europäische Kommission zwischen 2010 bis 2016 nichts unversucht um das Datenschutzbaby zustande zu bringen. Im April 2016 war es soweit, die DSGVO wurde beschlossen, jedoch noch zwei Jahre in den Brutkasten gelegt. Zeit genug für die EU-Staaten sich auf den neuen (Quäl?)geist einzustellen.

WAS SEITHER GESCHAH

Österreichs Politik löste die Aufgabe durchaus kreativ, wengleich wenig planvoll. Im Juni 2017 wurde das „Datenschutz-Anpassungsgesetz 2018" beschlossen. Noch vor Inkrafttreten wurden im April 2018 wesentliche Teile dieses Gesetzes in Form eines „Datenschutz-Deregulierungsgesetzes" wieder aufgehoben. Pünktlich mit 25. Mai 2018 brachte Max Schrems mehrere Datenschutzbeschwerden ein, Ergebnisse liegen bis heute keine vor. Pünktlich mit 25. Mai 2018 trat die „Datenschutz-Folgenabschätzung-Ausnahme-Verordnung" in Kraft. Hinter diesem Wortungetüm verbirgt sich eine lange Liste von Verarbeitungen, bei denen eine Art DSGVO-light gilt. Dann war Sommerpause. Erst im November wurde eine „Datenschutz-Folgenabschätzung-Verordnung" in Kraft gesetzt, die mehr Fragen als Antworten aufwirft.

DATENSCHUTZ-GRUNDVERORDNUNG WIRD UNWORT DES JAHRES 2018

Im Dezember erlebte die DSGVO ein neues, eher unrühmliches Hoch. Es wurde zum Unwort des Jahres 2018 und steht damit in einer Reihe mit „Negerkonglomerat", „Analogkäse" oder „Komasaufen". Eine Auszeichnung, die das ambivalente Verhältnis Österreichs zur modernen Informations- und Datengesellschaft treffend beschreibt.

DIE NEBEL LICHTEN SICH!

Die Datenschutzbehörde hat auch mit ihrer Tätigkeit begonnen, etwa 1000 Beschwerden langten ein, dazu gab es bisher etwa 100 Entscheidungen und vier Strafen. Sogar 551 Datenschutzverletzzungen wurden der Behörde gemeldet. Angesichts der täglich verlorenen USB-Sticks, Notebooks und Dateien eine viel zu kleine Zahl.

Mit den ersten Entscheidungen der Datenschutzbehörde beginnt auch so etwas wie gefühlte Rechtssicherheit um sich zu greifen. Im Datenschutz-Stenogramm haben wir die wichtigsten Punkte aufgelistet. Die meisten Entwicklungen waren erwartbar. Auch nach Start der DSGVO sind Werbeanrufe verboten, Mitgliedsanträge dürfen keine versteckten Zustimmungen enthalten und Video-Überwachungen sind weiterhin anzukündigen.

Neu ist hingegen, dass das Auskunftsrecht weder durch Geschäftsbedingungen oder Gesetze beschränkt werden darf. Dies hat sich ein findiger Bankkunde zunutze gemacht und statt der kostenpflichtigen Kontoauszüge schlicht eine Datenschutzauskunft verlangt.

Apropos Videoüberwachung (jetzt: Bildaufzeichnung), hier hat die Datenschutzbehörde auch strafmäßig „zugeschlagen", wenn auch sehr moderat. Die publizierten Strafen waren 4.500,- bzw. 6.700,- Euro. Es wirkt ein symptomatisch, wenn sich die österreichische Datenschutzbehörde vorrangig mit Videoüberwachung beschäftigt. „Hier hängt die Kamera, da fehlt das Hinweisschild", scheint das obere technische Niveau der Behörde zu sein.

KLARES DATENSCHUTZSIGNAL KOMMT AUS FRANKREICH

Das es auch anders geht hat die französische Datenschutzbehörde CNIL im Jänner 2019 gezeigt. Google wurde gleich zu 50 Millionen Euro Strafe wegen intransparenter Nutzungsbestimmungen „verdonnert".

BILDUNG WEITERHIN SCHLUSSLICHT IN DER INFORMATIONSGESELLSCHAFT

„Von einem heute 50-jährigen Lehrer könne man nicht dieselbe Internetkompetenz erwarten, wie von den 10-14-jährigen", meinte vor einigen Wochen ein sogenannter Bildungsexperte. Übersehen hat der famose Experte, dass bei der flächendeckenden Einführung des Internets im Jahr 1994 der heute 50-jährige altersschwache Lehrer 25 Jahre alt war, gerade mit der Ausbildung fertig war oder sogar noch mitten drin. Es wäre ihm wohl zumutbar gewesen damals sich ein wenig von der Informationstechnik anzueignen.

Während im Bildungssektor offenbar auch nach 25 Jahren Internet noch darüber gerätselt wird, ob „Internet" bloß ein vorübergehender grippaler Infekt ist oder doch massiv ansteckend ist, gehen die österreichischen Schulen ihre eigenen - eigenwilligen - Datenschutzwege. Immer mehr Schulen verwalten eMails, Schüler- und Lehrerdaten bei Google.

Bildungsminister Fassmann damit konfrontiert streitet jede Verbindung von Schulen mit Google ab, offenbar weiß er längst nicht mehr, was in seinem Wirkungsbereich passiert. Er ist aber nicht allein, auch zahlreiche andere Behörden, Anwaltskanzleien oder Ärzte vertrauen auf Google und schicken sensible Daten ihre Kunden, Klienten und Parteien ungefragt und ohne Absicherung dorthin.

Trotz der nicht gerade berauschenden Zukunftsaussichten wünsche ich allen ein erfolgreiches Datenschutzjahr!

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

ARGE DATEN

AUFREGER DES JAHRES

NAMENSSCHILDER AN GEGENSPRECHANLAGE

DSGVO garantiert Anonymität in allen persönlichen Lebensbereichen - auch die Tatsache wo jemand wohnt ist eine schutzwürdige Information - Namensangaben an Gegensprechanlagen sind nur mit Zustimmung des betroffenen Mieters/Wohnungseigentümers zulässig - eine Verpflichtung im Mietvertrag oder im Wohnungseigentümervertrag wäre DSGVO-widrig

Gemäß Datenschutzgrundverordnung (DSGVO) dürfen persönliche Daten nur zu konkreten Zwecken und auf Grund genau definierter gesetzlicher Vorgaben verarbeitet werden.

Für das Anbringen des Namens eines privaten Mieters oder Eigentümers an der Gegensprechanlage muss der Betroffene freiwillig zustimmen. Es gibt keine sonstigen rechtlich zulässigen Möglichkeiten. Hat eine Hausverwaltung die Zustimmung nicht eingeholt, ist das Anbringen DSGVO-widrig und kann sowohl mit Verwaltungstrafe als auch Schadenersatz belegt werden. Diese Verpflichtung zur Anonymität ist nicht neu und gilt seit 1980, seit Mai 2018 sind jedoch die Sanktionsmöglichkeiten verschärft. Wird der Anspruch auf Anonymität im höchstpersönlichen Lebensbereich ignoriert, kann Beschwerde bei der Datenschutzbehörde eingelegt werden. Das ist ein eher „zahnloses" Verwaltungsverfahren, dass relativ langwierig ist und für die Betroffenen in der Regel keinen unmittelbaren Nutzen hat.

Wesentlich effizienter ist das Einbringen einer Unterlassungs- und Schadenersatzklage beim Zivilgericht. Die meisten Rechtsschutzversicherungen finanzieren auch derartige Schadenersatzklagen. Mit dem Anbringen des Namens in einem öffentlichen Bereich ohne ausreichende Zustimmung erfolgte eine Datenschutzverletzung.

Besonders „schlaue" Hausverwaltungen / Vermieter versuchen eine fehlende Zustimmung durch Klauseln in den Mietverträgen zu sanieren. Dies wäre jedoch eine unzulässige Koppelung eines Zweckes (Wohnungsmiete) mit einem anderen Zweck (Offenlegung des persönlichen Lebensbereiches). Eine derartige Koppelung ist gemäß DSGVO verboten und unwirksam.

ANLASSFALL WIENER WOHNEN

Eine Beschwerde eines Gemeindebaumieter hat im vergangenen Jahr dazu geführt, dass die Türschilder bei Gegensprechanlagen aller 220.000 Gemeindebauwohnungen getauscht werden sollten. Wiener Wohnen begann mit dem Austausch, beendete diesen jedoch nach kurzer Zeit wieder und entschloss sich, die Namensschilder zu erhalten. Dabei beruft sich Wiener Wohnen auf ein bisheriges Fehlen der entsprechenden Judikatur aufgrund der kurzen Geltungsdauer der DSGVO.

AUSBILDUNGSREIHE „BETRIEBLICHER DATEN-SCHUTZBEAUFTRAGTER“

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

DATENSCHUTZ-LEHRGANG ERHÖHT WETTBEWERBSFÄHIGKEIT!

Datenschutz muss heute in Informationsprozesse integriert sein. Dazu ist es erforderlich alle Verarbeitungsschritte nachvollziehbar zu dokumentieren und grundrechtskonform zu gestalten. „Datenschutz“ ist damit ein integrales Element der Informationsprozesse, vergleichbar ausreichender Hardware-Ausstattung, einer modernen Internet- und Telekommunikations-Anbindung oder benutzerfreundlicher Softwaregestaltung. Wird diese Integration verabsäumt droht den Unternehmen ein immer größerer Rückstand gegenüber den US-Informationskonzernen.

DATENSCHUTZ-LEHRGANG MIT INTEGRATIVEM ANSATZ

Genau auf die Integration in die Informationsverarbeitung legt der ARGE DATEN Lehrgang größten Wert. Ganz im Gegensatz zu manchen Pseudo-Kursen, die Datenschutz auf Ausfüllen von Formularen, Einkauf von Datensicherheit oder möglichst raffinierte Geschäftsbedingungen reduzieren.

DATENSCHUTZ ERFORDERT TECHNISCHE UNTERSTÜTZUNG

Moderne Datenschutzanforderungen lassen sich ohne technische Unterstützung nicht bewältigen. Authentisierungsverfahren, Integritätsmaßnahmen, Design-Konzepte, Risiko-Analysen und smarte Lösungen für Langzeitarchivierung sind notwendig. Alle diese Themen werden im Lehrgang behandelt.

AUF DATENSCHUTZANFORDERUNGEN RICHTIG REAGIEREN

Kunden, Mitarbeiter, Konsumenten werden selbstbewusster. Sogenannte „GDPR-Nightmare-Letter“ geistern durch das Internet. Kompliziert formulierte „Datenschutz-Alptraum-Briefe“, deren Beantwortung Unternehmen lahmlegen könnten. Faktum ist, vieles in diesen „Briefen“ muss nicht beantwortet werden, vieles ist nur bürokratische Phantasie. Auf Datenschutzanfragen rasch, effizient und richtig reagieren, das ist in Zukunft ein wichtiges Geschäft des Datenschutz-Verantwortlichen. Der Lehrgang zeigt wie es geht.

WENIGER BÜROKRATIE MEHR VERANTWORTUNG

Mit der DSGVO können Datenverarbeiter flexibler als bisher persönliche Daten verarbeiten. Sie müssen keine bürokratischen Meldungen durchführen. Jeder Betrieb entscheidet, wie er mit persönlichen Daten umgeht und zu welchem Zweck er sie verwendet. Die Verarbeitung muss FAIR, TRANSPARENT und gemäß dem Minimalitätsprinzip erfolgen. Das erfordert laufend internes Datenschutzmanagement und Datenschutzfolgenabschätzung statt sinnleerer Formularwirtschaft.

VORTEIL EINES DATENSCHUTZ-VERANTWORTLICHEN

Jedes Unternehmen MUSS einen Datenschutz-Verantwortlichen haben. Die Aufgaben des Datenschutz-Verantwortlichen sind vielfältig: er informiert die Geschäftsleitung und die Mitarbeiter, berät bei der Datenschutz-Folgenabschätzung, koordiniert und setzt notwendigen Datenschutzmaßnahmen im Unternehmen um, koordiniert Fristen und Verpflichtungen, gemäß DSGVO. Er ist Ansprechperson für die Datenschutzbehörde.

ERFAHRUNG ZÄHLT - GANZ BESONDERS BEIM DATENSCHUTZ

Seit 2006 organisiert die ARGE DATEN mit großem Erfolg die Ausbildungsreihe „betrieblicher Datenschutzbeauftragter“ (mehr als 650 Absolventen und über 3500 Teilnehmer an unseren Modulen).
Die Vortragenden des Lehrgangs sind namhafte Experten aus Universität und Wirtschaft. Auf diese Weise kann fundiertes Fachwissen und klarer Praxisbezug garantiert werden. Die Ausbildungsreihe wird laufend an neue Entscheidungen und Entwicklungen angepasst.

DAS RICHTIGE BEIM DATENSCHUTZ TUN!

Der Lehrgang der ARGE DATEN behandelt Planung, Umsetzung und Tagesgeschäft des Datenschutz-Verantwortlichen. Mit der praxisnahen Ausbildung zum betrieblichen Datenschutzbeauftragten sind Sie bestens auf die neuen Herausforderungen vorbereitet.

MODULARE AUSBILDUNGSREIHE

Der Lehrgang besteht aus fünf in sich abgeschlossenen Modulen, die laufend angeboten werden. Die ersten vier Module können zu beliebigen Zeiten besucht werden, das Abschlussmodul ist ein Intensiv-Workshop und setzt den Besuch der anderen vier Module voraus. Hier kann das erworbene Wissen aktiv umgesetzt werden. Durch den Lehrgang erhalten unsere Teilnehmer Lösungsstrategien für höchst unterschiedliche Datenschutzfragen.

ZUSÄTZLICH ISO-ZERTIFIKAT ISO/IEC 17024 „DATENSCHUTZBEAUFTRAGTER“

Auf Wunsch kann direkt im Anschluss am Workshop die Prüfung zum ISO-zertifizierten ‚Datenschutzbeauftragten‘ gemäß Kriterien der ISO/IEC 17024 abgelegt werden. Nach bestandener Prüfung erhalten Sie von Autrian Standards ein Zertifikat und das Recht das Konformitätszeichen ‚Certified by Austrian Standards‘ zu verwenden. Das Zertifikat ist drei Jahre gültig. Die Prüfung ist ein Multiple-Choice-Test und dauert 1 1/2 Stunden.

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 neuen österreichischen Datenschutz-Gesetz (DSG).

MODUL II: DATENVERWENDUNG IM UNTERNEHMEN

Die Veranstaltung konzentriert sich auf die besonderen betrieblichen Datenschutzanforderungen. Bei umfassendem Einsatz von Internettechniken ergibt sich die Verpflichtung Betriebsvereinbarungen abzuschließen, weiters sind Informationspflichten nach dem eCommerceGesetz u. Mediengesetz zu beachten.
Diese Veranstaltung kann ohne besondere Vorkenntnisse besucht werden, empfohlen wird jedoch die Absolvierung der Veranstaltung „Modul I: Datenschutz Grundlagen" oder einer vergleichbaren Einführung in das Datenschutzrecht.

MODUL III: DATENSCHUTZ UND IT-SICHERHEIT

Anforderungen, Konzepte, Umsetzung
Die Tagesveranstaltung informiert über organisatorische und technische Anforderungen zur IT-Sicherheit, Sicherheitsstandards, Basissicherheit und Erweiterungen, Konzepte und Umsetzung von IT-Sicherheit, Grundlagen einer optimalen Security Policy.
Diese Veranstaltung kann ohne besondere Vorkenntnisse besucht werden, empfohlen wird jedoch die Absolvierung der Veranstaltung „Modul I: Datenschutz Grundlagen" oder einer vergleichbaren Einführung in das Datenschutzrecht.

MODUL IV: DATENSCHUTZ-GRUNDVERORDNUNG & PRAXIS

Die Themenschwerpunkte des eintägigen Seminars sind Erfahrungen von betrieblichen Datenschutzbeauftragten, europarechtliche Grundlagen des Datenschutzes, Melde- und Genehmigungspflicht im internationalen Datenverkehr.
Diese Veranstaltung kann ohne besondere Vorkenntnisse besucht werden, empfohlen wird jedoch die Absolvierung der Veranstaltung „Modul I: Datenschutz Grundlagen" oder einer vergleichbaren Einführung in das Datenschutzrecht.

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

MODUL V: WORKSHOP: DATENSCHUTZFRAGEN IM BETRIEB IDENTIFIZIEREN UND LÖSEN

Das Abschlussmodul zur Ausbildungsreihe „betrieblicher Datenschutzbeauftragter" gibt Gelegenheit auf praktische Datenschutzfragen einzugehen. Die Teilnehmer entwickeln und präsentieren selbst an Hand von anonymisierten Fallbeispielen optimale Lösungsstrategien.
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.

TÄTIGKEITSBERICHT ARGE DATEN 2018/19

Beispiele aus der Beratungspraxis der ARGE DATEN

- **Gemeinden:** Veröffentlichung von Gemeinderatssitzungsprotokoll
- **Gesundheit:** Opt-Out-Möglichkeiten bei ELGA
- **Bonität:** Löschung veralteter oder irreführender Bonitätsdaten
- **Statistik:** Verpflichtung zur Teilnahme an Mikrozensuserhebungen
- **DSGVO:** Informations- und Auskunftsrechte Betroffener
- **Behörden:** Möglichkeiten der Selbstauskunft
- **Gemeinden:** Veröffentlichungsrechte von Bürgerdaten
- **Arbeit:** Ausgabe von personalisierten Geschenkgutscheinen
- **Gesundheit:** Verwendung von Patientendaten zu klinischen Prüfungen, Forschungs- und Unterrichtszwecken
- **Arbeit:** Umgang mit Bewerbungsunterlagen
- **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 von der ARGE DATEN umfangreiche und kritische Stellungnahmen 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
2018/19 absolvierten 45 Teilnehmer den Lehrgang zum Datenschutzbeauftragten. Seit Beginn haben bisher mehr als 650 Personen den Lehrgang abgeschlossen.

An Datenschutzveranstaltungen von ARGE DATEN oder teilweise von ARGE DATEN organisiert, nahmen im Jahr 2018/19 in Summe rund 1.200 Personen teil.

DATENSCHUTZAUDIT GEMÄSS DSGVO

DSGVO Art 5, 6, 42, 43
Audit von Verarbeitungen reduziert Unsicherheiten in der Umsetzung der DSGVO - Vorbereitung auf künftige Datenschutzzertifizierung gemäß Art 42 - hohe Nachweispflichten zentrale Herausforderung für Verantwortliche und Auftragsverarbeiter - Österreichisches Normungsinstitut arbeitet an Datenschutz-Audit-Norm, die e-commerce monitoring Gmbh ist an der Formulierung beteiligt

DSGVO BRINGT WENIGER BÜROKRATIE UND MEHR VERANTWORTUNG

Im Grunde sind die Vorgaben der Datenschutzgrundverordnung (DSGVO) simpel und erlauben Informationsverarbeitern weitgehende Gestaltungsfreiheit.

Die DSGVO verlangt die „grundrechtskonforme Gestaltung aller personenbezogener Informationsprozesse".

Die neuen Gestaltungsmöglichkeiten der DSGVO werden jedoch durch mehr Unsicherheit erkauft. Die Datenschutzbehörde hat schon angekündigt keine Empfehungen und Hilfen zur Umsetzung der DSGVO zu geben. Viele Verantwortliche scheuen sich daher alle Möglichkeiten der DSGVO zu nutzen, zum Nachteil ihrer Wettbewerbsfähigkeit.

Technische Maßnahmen, wie revisionssichere Dokumentation, elektronische Signatur wichtiger Dokumente, qualifizierter Zeitstempel kritischer Prozesse sichern die Anforderungen der DSGVO ab. Externe Audits mit Erfahrungen bei der Gestaltung von sicheren Informationsprozessen können Unsicherheiten drastisch reduzieren.

GROSSE GESTALTUNGSMÖGLICHKEITEN BEI DEN VERWENDUNGSZWECKEN

Gerade Art 6 Abs 4 DSGVO bietet Verantwortlichen weitgehende Freiheit, zu welchen Zwecken sie persönliche Daten verarbeiten. Nicht nur zu ursprünglichen Zwecken dürfen persönliche Daten verwendet werden, sondern zu beliebigen anderen legitimen Zwecken, wenn eine ausreichende Folgenabschätzung gemacht wird.

Kriterien, die bei Wechsel des Verarbeitungszwecks zu beachten sind:
a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,
d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Ergibt eine gründliche Folgenabschätzung die Zulässigkeit der Verarbeitung zum neuen Zweck, dürfen die Daten dazu verwendet werden. Im Normalfall ohne weitere Zustimmung des Betroffenen, jedoch mit Benachrichtigung gemäß Art 13 oder 14.

Die Krux dieser neuen Freiheit ist, kaum jemand hat Erfahrung mit einer derartigen Abschätzung. Die Datenschutzbehörde hat schon jetzt angekündigt Verantwortliche dabei NICHT zu unterstützen. Externe Audits können dazu Rechtsunsicherheiten reduzieren.

ACCOUNTABILITY UND KONTINUITÄT SIND DIE NEUEN HERAUSFORDERUNGEN

Weder Zweckbindung, Zustimmung oder Auskunftspflicht sind in der DSGVO wirklich neu. Diese Verpflichtungen gibt es, zum Teil wortident, schon seit Verabschiedung der Datenschutzrichtlinie 1995. Bisher wurden sie jedoch zu wenig beachtet. Die neuen Strafdrohungen führen zu höherer Beachtung, übersehen werden jedoch die wirklich gravierenden Neuerungen der DSGVO.

Belegbarkeit aller Prozesse, Prüfbarkeit, Kontinuitätsmanagement, Datenschutzmanagement und Riskoanalyse sind die großen Herausforderungen. Herausforderungen die ohne technische Unterstützung wohl nicht zu „stemmen" sein werden.

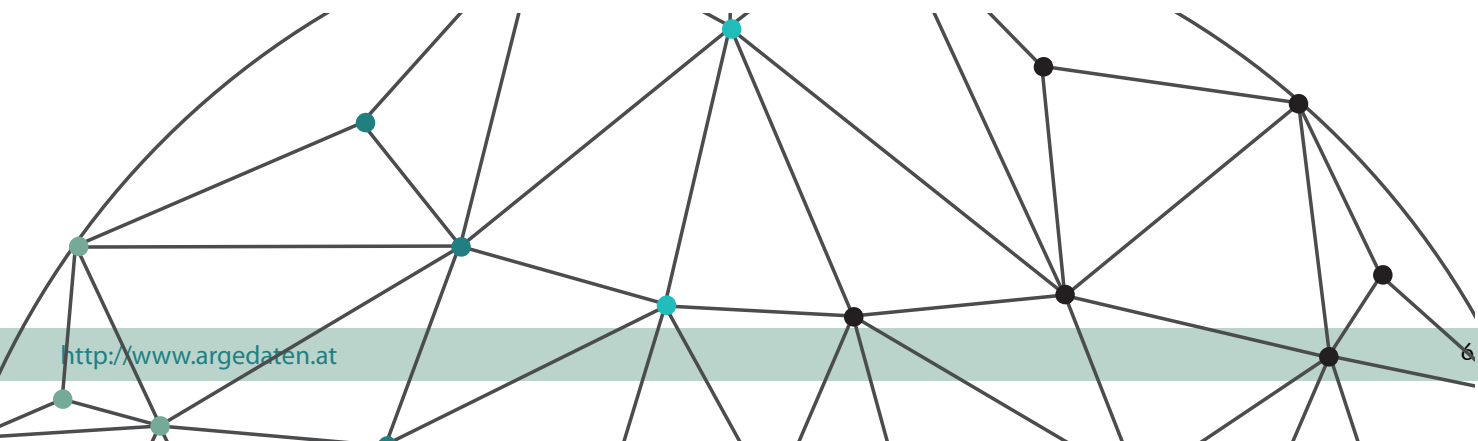
RECHENSCHAFTSPFLICHT („ACCOUNTABILITY")

Gemäß Art. 6 Abs 2 muss ein Verantwortlicher jeden Verarbeitungsschritt belegen können und bei Bedarf der Aufsichtsbehörde dokumentieren können. Jede Datenverarbeitung ist im Ergebnis so zu führen, als wäre jeden Tag ein - unangekündigtes - Audit möglich.

Ein regelmäßiges Audit, das bestätigt keine wichtigen Teile in der Rechenschaftspflicht vergessen zu haben, hilft Unsicherheiten zu beseitigen.

BELASTBARKEIT UND KONTINUITÄT („BUSINESS CONTINUITY MANAGEMENT")

Weitgehend unbemerkt wurden Belastbarkeit und Kontinuität bei der Verarbeitung personenbezogener Daten (DSGVO Art 32 Abs 1 lit b und c) zu datenschutzrelevanten Kriterien. In Zukunft hat ein Betroffener einer Datenverarbeitung den gesetzlichen Anspruch darauf, dass die Verarbeitung auch ausreichend verfügbar ist. Längere Ausfallszeiten müssen nicht mehr hingenommen werden und dürfen nicht mehr in Geschäftsbedingungen hineingeschrieben werden.



Vorfälle, wie in den letzten Jahren, bei denen in Österreich ein Onlinebanking-System mehrere Tage nicht verfügbar war oder in Großbritannien Operationen abgesagt werden mussten, weil die Rechner mit Schadsoftware verseucht waren, sind ab sofort auch als Datenschutzverletzung zu werten.

Selbst Gratisdienste werden in Zukunft eine bestimmte Verfügbarkeit sicherstellen müssen, ansonsten haben sie mit Schadenersatzklagen aus Datenschutzgründen zu rechnen.

Audits können helfen die Belastbarkeit von Systemen korrekt zu bewerten und die daraus resultierenden Risken zu minimieren. Weiters kann auf diese Weise sicher gestellt werden, dass tatsächlich regelmäßige Evaluierungen stattfinden.

RISIKOMANAGMENT („DATENSCHUTZ-FOLGENABSCHÄTZUNG")

Gemäß Art. 35 DSGVO ist für zahlreiche Verarbeitung eine Folgenabschätzung erforderlich. Insbesondere bei Einsatz neuer Technoilogien, wie Tracking- und Targetingverfahren, Big Data, biometrische Erkennung oder Internet-of-things-Anwendungen sind derartige risikobasierte Abschätzungen erforderlich.

Viele Verantwortliche sind jedoch unsicher die Sicht der Betroffenen ausreichend zu berücksichtigen. Viele fühlen sich „betriebsblind" was die Gefährdung Dritter durch die eigene Informationsverarbeitung betrifft, man wolle ja sowieso nur „das Beste für alle".

Auch für diesen Punkt hat sich externe Expertise bewährt. Der Blick „von außen" hilft Risken zu identifizieren, die ansonsten übersehen werden. Unangenehme Folgen, wie Strafverfahren und Schadenersatzforderungen können so vermieden werden.

DATENSCHUTZDESIGN („PRIVACY BY DESIGN")

Art. 25 DSGVO verlangt „Datenschutz durch Technikgestaltung", Verarbeitungen sollen so designed werden, dass die Vorgaben der DSGVO auf die einfachste Art und Weise erfüllt werden.

Dies bedeutet frühzeitige Anonymisierung, weitestgehende Pseudonymisierung, Verschlüsselung bei Archivierung und Datenübertragung, aber auch automatisierte Informations- und Auskunftsprozesse für den Betroffenen.

Vergleichbar einem Online-Bankkonto wäre daher eine „gute" Informationsverarbeitung ein System, bei der der Betroffene jederzeit Einblick in sein Datenkonto hat, diese Daten auch in portabler Form abspeichern kann und - soweit es seine Stammdaten sind, auch selbständig berichtigen kann. Auch benutzergesteuerte Löschprozesse fallen unter „Datenschutz durch Technikgestaltung".

Auch hier kann eine externe Sicht helfen, sinnvolle Maßnahmen gegenüber überflüssigen Mehraufwand klar abzugrenzen.

AUDITS ALS VORBEREITUNG EINER DATENSCHUTZZERTIFIZIERUNG

Mit Stand 25. Mai 2018 gibt es EU-weit noch keine anerkannten Zertifizierungsmechanismen gemäß Art. 42 DSGVO, aber es lassen sich schon wesentliche Grundzüge ableiten. Unter anderem arbeitet das Österreichische Normungsinstitut an entsprechenden Audit-Kriterien. Die e-commerce monitoring gmbh, als langjährig erfahrener Vertrauensdienstanbieter, ist in die Normenentwicklung eingebunden.

Es macht daher schon jetzt Sinn durch Audits festzustellen, ob man bei der Umsetzung der DSGVO „auf dem richtigen Weg" ist.

KONSEQUENZEN FEHLERHAFTER DSGVO-UMSETZUNG

Die meisten Informationsverarbeiter haben bis 25. Mai 2018 irgendetwas zur Umsetzung der DSGVO gemacht. Oft auf Grund der Empfehlungen ihrer Kammern, ihrer Aufsichtsstellen, von Anwälten oder IT-Lieferanten. Ob es das Richtige, das Notwendige und auch das Sinnvolle ist, ist in vielen Fällen ungewiss.

Niemand bestätigt derzeit, dass irgendwelche Dokumente auch tatsächlich im Zuge einer Beschwerde „halten". Schwerer wiegt jedoch die Frage, „wurden alle Gestaltungsmöglichkeiten der DSGVO genutzt?" Oder hat sich ein Verantwortlicher überflüssige Hürden auferlegt.

Hat ein Verantwortlicher zu wenig gemacht drohen einerseits Verwaltungsstrafen, die in Österreich „abgemildert" wurden, andererseits aber auch Schadenersatzklagen, die höchts unangenehm und teuer werden können. Steht eine Verarbeitung 5 Tage still, obwohl die Betroffenen damit rechnen, dass sie verfügbar ist, könnten rasch je Betroffenen 1.000.- und mehr Euro Schadenersatz, allein aus diesem Stillstand abgeleitet werden. Bei 20 oder 30.000 Betroffenen eine existenzbedrohende Angelegenheit.

Hat jedoch ein Verantwortlicher überflüssiges aus der DSGVO umgesetzt, hat er gegenüber seinen Mitbewerbern Wettbewerbsnachteile. Die können unter umständen teurer als jedes Verwaltungstrafverfahren sein.

WAS IST EINE GÜLTIGE EINWILLIGUNG (ZUSTIMMUNG) GEMÄSS DSGVO?

DSGVO Art 6-9, 49, 82, 83, TKG 2003 §§ 107, 109 Einwilligung eine Variante personenbezogene Daten zulässigerweise zu verarbeiten - Einwilligung ist in vertraglichen Verhältnissen von geringer Bedeutung - Kriterien einer gültigen Einwilligung: dokumentiert, korrekte Information („informed consent"), Freiwilligkeit, jederzeitige Widerrufbarkeit - Einwilligung bei elektronischen Marketingmaßnahmen wesentlich - DSGVO verlangt umfassende Dokumentationspflichten - bisherige Zustimmungen gelten auch nach 25. Mai 2018 - Empfehlungen für Versender und Bezieher

EINWILLIGUNG EINE FORM PERSONENBEZOGENE DATEN ZULÄSSIGERWEISE ZU VERARBEITEN

Art. 6 DSGVO listet für „normale" personenbezogene Daten gültige Kriterien einer rechtmäßigen Verarbeitung auf, Art. 9 DSGVO für den Bereich der besonderen Datenkategorien (früher: „sensible Daten"). In beiden Fällen ist Einwilligung eine von mehreren Möglichkeiten zur rechtmäßigen Verarbeitung.

Darüber hinaus ist Einwilligung auch von wesentlicher Bedeu-

tung, wenn Daten in unsichere Drittstaaten übermittelt werden sollen. Stimmt der Betroffene nach Aufklärung über alle Risken zu (Art. 49 DSGVO), kann die Übermittlung ohne weitere Sicherheitsvorkehrungen erfolgen.

KEINE FORMVORSCHRIFTEN FÜR EINWILLIGUNG

Grundsätzlich gibt es keine Formvorschrift, wie eine Einwilligung einzuholen ist. Ausdrücklich lässt die DSGVO zu, dass die Einwilligung mündlich, schriftlich oder durch bestätigende Handlung erfolgt.

So kann das Anklicken eines Kästchens bei einem Online-Formular eine gültige Einwilligung darstellen. Sogar das Versenden eines vorausgefüllten Kästchens kann eine gültige Einwilligung darstellen, wenn das Gesamtdesign eines Formulars so gestaltet ist, dass die Willenserklärung des Betroffenen eindeutig erkennbar ist.

Sicher keine gültige Einwilligung sind Erklärungen in den AGBs oder auf irgendwelchen Neben-Webseiten, wenn deren Kenntnisnahme nicht gesichert wird. Auch keine Einwilligung sind Schilder beim Eingang, an denen ein Betroffener üblicherweise ohne Kenntnisnahme vorbeigeht (Beispiel: „Mit Betreten des Raumes stimmt der Betroffene der Videoüberwachug zu“).

Auch nachträgliche Einwilligungserklärungen sind ungültig. So finden sich auf Konzertkarten auf der Rückseite Auszüge einer „Hausordnung“, bei denen man Fotos, Filmaufnahmen oder dergleichen „zustimmt“. Die Krux daran ist, dass diese Erklärungen erst nach Bezahlen, mit Zusendung der Karten zur Kenntnis gebracht werden. Das ist zu spät.

Ebenfalls keine gültige Einwilligung lässt sich aus „Gewohnheitsrecht“ oder dergleichen ableiten. Etwa: weil ein Betroffener seit mehreren Jahren unverlangten eMails nicht widersprochen hat, habe er - quasi durch Duldung - seine Einwilligung gegeben. Nicht reagieren ist jedoch, entgegen den Meinungen der WKO, keine bestätigende Handlung im Sinne der DSGVO.

Auf Grund der enormen Möglichkeiten die Einwilligungen für Verantwortliche bieten, ist die Gültigkeit einer Einwilligung daher gemäß DSGVO an strenge Vorgaben gebunden:

- Nachweispflicht
- korrekte Information („informed consent“)
- Freiwilligkeit
- jederzeitige Widerrufbarkeit

NACHWEISPFLICHT DER EINWILLIGUNG

Der Verantwortliche muss für die gesamte Dauer der Gültigkeit einer Einwilligung nachweisen können, dass er eine derartige Einwilligung erhalten hat. Gelingt der Nachweis nicht, drohen empfindliche Strafen. Es gibt jedoch auch keine Formvorschriften, wie dieser Nachweis auszusehen hat.

Hat jemand längere Zeit elektronische Zusendungen erhalten und darauf positiv reagiert, wird das auch als zustimmende Handlung anzusehen sein.

Bei unerwünschten Telefonanrufen oder bei Spam-Mails werden die Bestimmungen des TKG 2003 in Frage kommen, diese sehen Strafen bis 58.000,- Euro vor. In allen anderen Fällen werden die Strafen der DSGVO zur Anwendung kommen (bis 4% des Jahresumsatzes oder bis 20 Mio Euro).

Es gibt zwar keine Formvorschriften zum Nachweis der Einwilligung, langfristig werden jedoch revisionssichere Formen erforderlich sein, etwa durch Signatur der elektronischen Nachweise oder durch Verwendung qualifizierter Zeitstempel. Nur auf diese Weise können nachträgliche Manipulationen verhindert werden.

Einmal erteilte Einwilligungen können so lange aufbewahrt werden, als es für den Nachweis der Gültigkeit der Einwilligung erforderlich ist. Dies kann auch nach Widerruf einer Einwilligung notwendig sein.

EINWILLIGUNG ERFORDERT KORREKTE INFORMATION („INFORMED CONSENT“)

Eine Einwilligung ist nur dann gültig, wenn der Betroffene tatsächlich über den vollen Umfang welche Daten zu welchen Zweck verarbeitet werden informiert wurde. Er muss auch über alle möglichen Konsequenzen seiner Einwilligung, insbesonders über Sicherheitsrisken informiert werden.
Ein „Ersuchen um Einwilligung [muss] in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so

erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden [ist]" verlangt konkret Art. 7 Abs 2 DSGVO.

Damit wird eine Einwilligung auch dann ungültig, wenn sie langatmig in „Juristen-Kauderwelsch" abgefasst ist. 20 und mehr Seiten lange Erklärungen sind zumindest gegenüber Privatpersonen keine gültige Einwilligung. Es ist grundsätzlich zulässig über Datenschutzrechte und Verarbeitungen auch in einem langen Dokument zu informieren. Wesentliche Punkte, wie Einwilligung sollten gesondert, zu Beginn oder deutlich hervorgehoben zusammengefasst dargestellt werden.

EINWILLIGUNG MUSS FREIWILLIG ERFOLGEN

Es ist ebenfalls unzulässig eine Einwilligung mit anderen, sachfremden Sachverhalten zu verknüpfen. Auch derartige Erklärungen sind ungültig. Derzeit besteht jedoch große Unsicherheit, wann eine Verknüpfung einer Einwilligung mit anderen Sachverhalten sachlich gerechtfertigt ist und wann nicht.

So kann argumentiert werden, dass eine kostenlose Restaurant-App, die mir zeit- und ortsabhängige Restaurantvorschläge liefert, nur durch Nutzung der Standortdaten für Werbezwecke organisiert und finanziert werden kann. Die Einwilligung zur Nutzung persönlicher Daten zu Werbezercken kann daher nach genauer Information gültig sein.

Nicht gültig wäre jedoch eine Einwilligung, bei der eine Bank ein Girokonto nur dann eröffnet, wenn der Betroffene seine Sozialversicherungsnummer und seinen Familienstand bekannt gibt. Beides steht in keinem sachlichen Zusammenhang mit einem Girokonto.

EINWILLIGUNG KANN JEDERZEIT WIDERRUFEN WERDEN

Hat ein Verantwortlicher eine - nach den strengen Kriterien der DSGVO - gültige Einwilligung erwirkt, dann muss er mit dem jederzeitigen Widerruf einer Einwilligung rechnen. Derartige Widerrufe können völlig unbegründet und jederzeit erfolgen.

EINWILLIGUNG KEIN GEEIGNETES MITTEL PROZESSE ZU STEUERN

Auf Grund dieser engen Vorgaben sind Einwilligungen ungeeignet Pozesse zu steuern, seien das Arbeitsprozesse, Kunden-Lieferanten-Beziehungen, sonstige Industrie- oder Geschäftsprozesse, weder Bankkonten, noch Telekommunikationsdienste, Krankenbehandlungen oder Bestellungen könnten auf Basis von Einwilligung organisiert werden.

Faktum ist, dass in Bereichen mit hoher Qualität, hoher Betriebssicherheit oder Vertrauenswürdigkeit Einwilligung keine Bedeutung hat und vielmehr die vertragliche Gestaltung der Beziehung zwischen Verantwortlichen und Betroffenen im Vordergrund steht.

Im Rahmen von vertraglichen Vereinbarungen kann Widerruf ausgeschlossen werden oder führt schlicht zur Kündigung des Vertrages, mit beiderseitigen Konsequenzen. Gültig sind derartige Verträge jedoch ebenfalls nur dann, wenn sie nur die Verwendung notwendiger Daten vereinbaren. Auch bei Verträgen ist das Minimalitätsprinzip gemäß Art 6 DSGVO zu beachten. In welchem Umfang personenbezogene Daten „notwendig" sind, hängt von der Gestaltung einer Leistung ab.

So darf eine Versicherung den Abschluss einer Lebensversicherung nicht an der Einwilligung der Bekanntgabe von Sport- oder Rauchgewohnheiten binden. Es wäre aber sehr wohl zulässig, spezielle Sport- oder Raucherprodukte mit besonderen Konditionen anzubieten, bei denen die Bekanntgabe der Sport- oder Rauchgewohnheiten Teil des Versicherungsvertrages sind.

EINWILLIGUNG IM MARKETINGBEREICH VON ZENTRALER BEDEUTUNG

Von Bedeutung sind Einwilligungen im Sinne der DSGVO eigentlich nur im Werbe- und Marketingbereich. So dürfen Werbe-eMails und Massen-eMails nur mit Einwilligung des Betroffenen zugesandt werden. Eine Verknüpfung mit anderen Diensten ist unzulässig.

Ausschließlich bestehende Kunden, die im Zusammenhang mit einer Bestellung ihre eMail-Adresse bekannt gegeben haben, dürfen Werbung zu ähnlichen Produkten erhalten. Zumindest solange sie nicht widersprechen und sie nicht auf einer Sperrliste der RTR stehen.

Nur für diesen Bereich kann die Einwilligung durch Widerspruch ersetzt werden, ansonsten gelten: Verwendung von Daten zur elektronischen Werbung nur durch dokumentierte, informierte und freiwillige Einwilligung mit jederzeitiger Widerufsmöglichkeit.

BISHERIGE EINWILLIGUNGEN BLEIBEN GÜLTIG

Die gute Nachricht vornweg. Wer heute Werbemails und Newsletter mit einer gültigen Einwilligung verschickt, muss wegen der DSGVO nichts machen. Faktum ist, dass die „neuen" DSGVO-Bestimmungen nicht neu sind, sondern schon seit mehr als 10 Jahren im Rahmen der Anti-Spambedingungen des Telekommunikationsgesetzes (TKG 2003) gelten.

Im Zusammenhang mit den - scheinbar neuen und strengen - Einwilligungskriterien der DSGVO wurden viele Betreiber von eMail-Newslettern verunsichert.

„Habe ich wirklich eine ausreichend dokumentierte Einwilligung im Sinne der DSGVO", fragen sich viele. Manche Anwälte und die WKO empfehlen „zur Sicherheit" eine neue Einwilligung einzuholen.

IST ES SINNVOLL NACHTRÄGLICH EINWILLIGUNGEN EINZUHOLEN?

Faktum ist jedoch, in vielen Fällen bestand zu keinem Zeitpunkt eine gültige Einwilligung. Fehlt eine derartige Einwilligung, ist es auch nicht erlaubt jemanden per eMail / Telefon nur zum Zweck der Einwilligung zu kontaktieren.

Schon ein derartiges eMail/Telefonat wäre eine Verletzung der Spam-Bestimmungen und sollte unterbleiben.

Die ARGE DATEN empfiehlt Newsletter-Versender KEINE neuen Einwilligungsversuche zu starten, sondern darauf zu vertrauen, dass die bisherigen Einwilligungen ausreichen.

Nach bisherigen Erfahrungen ist die Rücklaufquote für derartige Einwilligungs-Spam-Mails weniger als 5%. Gleichzeitig gibt man jedoch einer sehr großen Zahl von Personen zu verstehen, dass man keine gültige Einwilligung hat. Dies könnte ab den 25. Mai 2018 etliche Personen motivieren Anzeigen nach §109 TKG 2003 oder Art. 83 DSGVO einzubringen oder Schadenersatzforderungen nach Art. 82 DSGVO zu erheben.

Wer ernsthaft an der Gültigkeit seiner eMail-/Telefonlisten zweifelt, sollte die entsprechende Personengruppe streichen und

auf dem Postweg, durch Webformulare, durch Preisausschreiben oder sonstige Aktivitäten motivieren, sich neu anzumelden.

Die ARGE DATEN empfiehlt Newsletter-Bezieher keine Einwilligungs-eMails zu beantworten, oft ist in den Einwilligungen zum Newsletterbezug auch der Versuch formuliert, andere Teile einer Geschäftsbeziehung zu „sanieren".

Wer ab 25. Mai 2018 unerwünschte eMails erhält, sollte dasselbe wie vorher tun, sich vom Newsletterbezug abmelden. Nur dort, wo das nicht funktioniert, ist eine Anzeige sinnvoll. Bei besonders hartnäckigen Fällen ist auch eine Schadenersatzforderung in der Höhe von etwa 1.000,- Euro („Missachtung der DSGVO") sinnvoll.

SCHADENERSATZ UND STRAFEN FÜR DATENSCHUTZVERLETZUNGEN

DSGVO 79, 82-83; DSG §§ 27, 29;
Nach Einschätzung der ARGE DATEN wird die Schadenersatzfrage in Zukunft von großer Bedeutung sein und daher die Zahl der zivilrechtlichen Schadenersatzklagen aufgrund von Datenschutzverletzungen zunehmen - materieller und immaterieller Schadenersatz möglich - Musterbeispiele bei denen Schadenersatz eingeklagt werden kann - Beschwerderecht bei Datenschutzbehörde - Bemessung der Höhe von Datenschutzstrafen

Nähere Informationen online unter: http://www.argedaten.at

DÜRFEN E-MAIL-INHALTE VON RECHTSVERTRETERN WEITERGEGEBEN WERDEN?

DSGVO Art 4, 6, 82-83; StGG §§ 10-10a;
Im Rahmen der Geltendmachung von Ansprüchen werden E-Mails vom Empfänger an seinen Rechtsvertreter weitergegeben. Dieser verschickt jedoch die E-Mails ohne Einwilligung des ursprünglichen Absenders unaufgefordert an Dritte (Personen, die weder Empfänger, noch Absender der E-Mail sind).

Die ARGE DATEN hat sich schon mehrfach mit der Problematik der Einordnung von E-Mails beschäftigt. Grundsätzlich wird bei unverschlüsselten Mails nicht von der Geltung des Briefgeheimnisses im engeren Sinn auszugehen sein (Art 10 Staatsgrundgesetz, StGG), sehr wohl jedoch von der Geltung des Fernmeldegeheimnisses (Art 10a StGG).

Weiters handelt es sich um Dateien, die, da sie zumindest Absender und Empfänger als personenbezogene Daten enthalten, unter die Bestimmungen der DSGVO fallen.

Als personenbezogen sind die Absende- und Zustell-Mailadresse anzusehen. Dies gilt selbst bei sogenannten Funktionsadressen, wie office@...., usw., auch diese wurden von Personen verfasst oder veranlasst. Hier liegt zumindest ein identifizierbarer Personenbezug vor, d.h. zumindest der Absender kann feststellen, welche Person der tatsächliche Verfasser ist. Identifizierbare (in Österreich: indirekt) personenbezogene Daten sind jedoch von der Geheimhaltung gleich zu behandeln wie sonstige personenbezogene Daten (Art 4 Zif 1 DSGVO).

Darüber hinaus enthalten die meisten Mails Signaturen mit den Kontaktdaten des Absenders, diese Daten sind jedenfalls personenbezogen. Damit sind diese Daten geheimhaltungswürdig gemäß DSGVO, ein Abgehen von der Geheimhaltung ist daher an die Bestimmungen des Datenschutzrechtes gebunden.

Der rechtmäßige Empfänger eines E-Mails wird den Inhalt dann weitergeben bzw. veröffentlichen dürfen, wenn dies zur ‚Wahrung überwiegender berechtigter Interessen' gemäß Art 6 Abs 1 lit f DSGVO notwendig ist. Fühlt sich etwa jemand durch ein E-Mail in seinen Rechten verletzt, dann wird er das E-Mail seinem Rechtsvertreter oder auch gegenüber den zuständigen Behörden/Gerichten vorlegen dürfen.

Diese Stellen sind jedoch ihrerseits zur Geheimhaltung verpflichtet, sei es aus Gründen des Amtsgeheimnisses, beruflicher Geheimhaltungsverpflichtungen oder aus den Geheimhaltungsverpflichtungen gemäß DSGVO. Eine Weitergabe wird daher ebenfalls nur zulässig sein, wenn sie zur ‚Wahrung überwiegender berechtigter Interessen' notwendig ist. Dies kann bei einem Rechtsvertreter nicht weitergehen, als bei beim eigentlichen Beschwerdeführer.

Eine Weitergabe von E-Mails oder gar deren Veröffentlichung aus Demonstrationsgründen wird jedenfalls unzulässig sein. Wird jemand ungewollt zum Empfänger derartiger E-Mails, dann ist er verpflichtet diese ‚nicht zur Kenntnis zu nehmen'. D.h. er wird das E-Mail solange durchlesen dürfen, bis er erkennen kann, dass es Informationen enthält, die nicht für ihn bestimmt sind. Aus Beweissicherungsgründen darf ein derartiges Mail auch aufgehoben werden, die Inhalte dürfen jedoch nicht verwendet werden. Eine Weitergabe des anonymisierten Mailinhalts an Dritte wird jedoch zulässig sein.

WANN SIND DATEN RECHTMÄSSIG VERÖFFENTLICHT?

DSGVO Art 5-6, 19, 82-83 DSG §§ 22, 24
Bei strenger Auslegung des Schutzes der Privatsphäre sind viele Veröffentlichungen persönlicher Daten im Internet unrechtmäßig

Geben Sie einen beliebigen Familien- und Vornamen im Internet ein und Sie werden jede Menge von Listen mit persönlichen Daten erhalten.
Egal ob Telefonbucheinträge, Lebensläufe, Klassen- oder Studienlisten, Ergebnislisten bei Sportveranstaltungen, Veranstaltungsteilnamen, Biographien und Zitiersammlungen, Lehrer- und Schülerbewertungen, Bewerberlisten, Mitarbeiterdaten oder Abrechnungen von Hausverwaltungen.
Warnlisten über Personen und Unternehmen finden sich genauso darunter, wie Listen von Globalisierungskritikern, Teilnehmern an internen eGovernment-Seminaren oder Einladungslisten von Pfarrkränzchen.

Weblogs mit fragwürdigen Inhalten oder die Kaffeehaus-Webcam runden das alltägliche Bild vom privaten Lauschangriff und Datenmissbrauch ab.

Meist sind es nur winzige Informationssplitter über eine Person, nicht geeignet für systematische Überwachungen, aber oft ausreichend, um Einblicke in persönliche Meinungen und Privatleben von einzelnen Menschen zu erhalten.

OFT UNRECHTMÄSSIGE VERÖFFENTLICHUNGEN

Eine rechtmäßige Veröffentlichung im Internet gemäß DSGVO liegt nur dann vor, wenn der Grundsatz der Zweckbindung erfüllt ist und ein Rechtfertigungsgrund oder eine Einwilligungserklärung gegeben ist. Fehlt eine, dann ist die Veröffentlichung unrechtmäßig.

RECHTFERTIGUNGSGRUND ODER EINWILLIGUNGSERKLÄRUNG

Die DSGVO verlangt zumindest einen der folgenden Rechtfertigungsgründe für die rechtmäßige Datenverarbeitung, sofern keine Einwilligungserklärung für einen oder mehrere bestimmte Zwecke vorliegt (Art 6 Abs 1 DSGVO):

(1) Die Veröffentlich ist für die Erfüllung eines Vertrags, dessen Vertragspartei der Betroffene ist oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage des Betroffenen erfolgen.
(2) Die Veröffentlichung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.
(3) Die Veröffentlichung schützt lebenswichtige Interessen des Betroffenen oder eines Dritten.
(4) Die Veröffentlichung schützt überwiegende berechtigte Interessen des Kindes.
(5) Die Veröffentlichung schützt berechtigte Interessen des Verantwortlichen oder eines Dritten.
(6) Die Veröffentlichung dient öffentlichen Interessen.

EINWILLIGUNG DES BETROFFENEN

Wer keine Rechtfertigung für eine Aufnahme vorweisen kann, braucht die Einwilligung der betroffenen Person. Diese muss der Veröffentlichung ihrer personenbezogenen Daten für einen oder mehrere bestimmte Zwecke zustimmen und zudem über Zweck und Umfang der Veröffentlichung aufgeklärt sein. Generaleinwilligungserklärungen gab es nie und gibt es mit der DSGVO gleich gar nicht.

Selbst wenn die Veröffentlichung einem berechtigten Zweck folgen würde bedarf die Veröffentlichung im Internet der Einwilligung durch den Betroffenen (Art 6 Abs 1 lit a DSGVO). Eine Einwilligung, die ausdrücklich zu erteilen ist, jederzeit widerrufen werden kann und nicht bloß konkludent - etwa durch Teilnahme an einer Veranstaltung - erfolgen kann. Niemand muss damit rechnen, dass er, nur weil er an einer Sportveranstaltung oder einem Bildungsangebot teilgenommen hat, im Internet veröffentlicht wird. Eine derartige Einwilligung muss „in Kenntnis der Sachlage und frei von jedem Zwang" erfolgen.

BERECHTIGTER ZWECK

Jede Veröffentlichung muss gemäß Art 5 Abs 1 lit b DSGVO einem berechtigten Zweck (Zweckbindungsgrundsatz) verfolgen, etwa die Information von Teilnehmern untereinander oder die Information der Öffentlichkeit über bestimmte Ergebnisse (etwa bei Sportveranstaltungen). Ein derartiger berechtigter Zweck ist aber in vielen Fällen nicht gegeben. Wenn etwa die Teilnahme an einem Seminar dokumentiert wird, interessiert dies, abgesehen von den Teilnehmern, niemand. Ganz im Gegenteil besteht für die Teilnehmer ein Schutzanspruch, dass nicht jeder von der Teilnahme erfährt, und sei es nur um unerwünschte Werbung zu verhindern. Zur bloß internen Kommunikation untereinander ist aber eine frei zugängliche Liste unzulässig, hier wären nur interne, passwortgesicherte Listen erlaubt.

DATENSCHUTZVERLETZUNGEN SIND DEN MEISTEN MENSCHEN NICHT BEKANNT

Tatsächlich sind die meisten Internet-Datenschutzverletzungen den Betroffenen nicht bekannt. Sie rechnen schlicht und einfach nicht damit mit ihrem Namen im Internet aufzuscheinen.

DSGVO VERLANGT AUFSICHT DURCH NATIONALE DATENSCHUTZBEHÖRDE

Obwohl der Schutz der Privatsphäre eine höchstpersönliche Angelegenheit ist, kann der Bürger auch darauf vertrauen, dass sein Schutz durch Behörden wahrgenommen wird.

Aus diesem Grund verlangt die DSGVO (http://ftp.freenet.at/privacy/ds-at/dsg2018-aktuell.pdf) eine nationale unabhängige Datenschutzbehörde, die die Einhaltung der allgemeinen Datenschutzregeln verlangt. In Österreich wäre dies nach dem DSG zwar die Datenschutzbehörde, diese hätte auch gemäß §§ 22 und 24 DSG das Recht der Überprüfung von Datenverarbeitern auf Einhaltung der Datenschutzbestimmungen. Dies geschieht jedoch gerade im Zusammenhang mit Veröffentlichungen im Internet praktisch nie. Sollte es an Kapazität mangeln stellt die ARGE DATEN gern eine Liste von Links zur Verfügung, bei denen die Rechtmäßigkeit der Veröffentlichung persönlicher Daten zumindest zweifelhaft und jedenfalls prüfwürdig ist.

VERSTÄNDIGUNGSPFLICHT BEI BERICHTIGUNG UND LÖSCHUNG

Wie soll sich jedoch ein Internetnutzer korrekt verhalten? Daten die rechtmäßig veröffentlicht sind, darf er zu seinen berechtigten Zwecken nutzen, unrechtmäßig veröffentlichte Daten darf er weder nutzen, noch weitergeben, er darf sie strenggenommen, gar nicht „zur Kenntnis nehmen".

Alle rechtswidrigen Veröffentlichungen sind unverzüglich zu löschen. Weiters müssen Verantwortliche alle Empfänger, an den er die rechtswidrig veröffentlichten Daten weitergegeben haben, über die Löschung informieren (Art 19 DSGVO). Die DSGVO normiert damit auch eine umfassende Mitteilungspflicht.

MÜSSEN IM RAHMEN EINER SOGENANNTEN ‚SELBSTAUSKUNFT' DATEN AN DEN KSV ÜBERMITTELT WERDEN?

DSGVO Art 15-17, 21
Selbstauskünfte an den KSV sind freiwillig und müssen nicht erteilt werden. Die ARGE Daten rät, keine Auskünfte zu erteilen und im Gegenzug selbst ein Auskunftsbegehren an den KSV zu stellen.

Nähere Informationen online unter: http://www.argedaten.at

WAS DARF/MUSS EIN VERANTWORTLICHER ZUR AKTUALISIERUNG VON PERSONENBEZOGENEN DATEN TUN?

DSGVO Art 12, 16-17, 82-83
Eine aktive Aktualisierungspflicht, also das selbständige Nachforschen, ob Informationen noch richtig sind, wird einem Verantwortlichen - abhängig vom Zweck - im wirtschaftlich zumutbaren Ausmaß zukommen - Fehlerhafte Daten müssen richtiggestellt werden, unvollständig Daten müssen ergänzt werden - Im Falle von Datenschutzverletzungen drohen Sanktionen

Ein Betroffener kann die Löschung, Richtigstellung oder Aktualisierung verlangen. In diesem Fall muss dem Wunsch unverzüglich, jedenfalls aber binnen eines Monates entsprochen werden oder es muss begründet werden, warum dem Wunsch nicht entsprochen wird (Art 12 DSGVO).

Grundsätzlich ist kein Verantwortlicher verpflichtet, täglich alle Informationen aktiv nach ihrer Gültigkeit zu überprüfen. Jeder Verantwortliche ist aber verpflichtet ein technisches und organisatorisches System zu entwickeln, dass die Aktualisierungen im notwendigen Ausmaß sicherstellt.

Viele seriöse Verantwortliche stehen vor dem Problem die Aktualisierungspflichten gemäß Art 17 DSGVO angemessen zu erfüllen. Es sind viele Unternehmen von sich aus interessiert (Vermeidung von Portokosten, Streuverluste in der Werbung, ...) ‚Karteileichen' und doppelte Datensätze zu erkennen und zu entfernen.

Für die Aktualisierungsarbeiten von Daten sind Auswertungs- und Abgleichprogramme, die etwa phonetische Unterschiede erkennen und entfernen, jedenfalls zulässig. Sicher zulässig ist es auch, verschiedene eigene, bisher getrennte Datenbestände eines Geschäftsbereiches miteinander zu verknüpfen und abzugleichen. Auch eigene Recherchen, wie Telefonanrufe bei eingetragenen Kunden und Interessenten, schriftliche Anfragen, Online-Recherchen, die Auswertung von veröffentlichten Telefonanschlussdaten (=Telefonbücher) oder auch der Zukauf von Adressen, etwa von der Wirtschaftskammer (Geschäftsdaten) oder von einem Adressenverlag werden erlaubt sein.

Problematisch wird es bei der Benutzung öffentlich-rechtlicher Datenbestände, also Informationen, die für gänzlich andere Zwecke vorgesehen sind, etwa die Meldeevidenz, die Wählerevidenz oder die Grundstücksdatenbank. Im Zuge gezielter Abfragen nach bestimmten Personen wird es auch hier zulässig sein, diese Daten zur Aktualisierung eigener Informationen zu verwenden, eine generelle Übernahme dieser Daten und eines Abgleichs mit den eigenen Informationen wird jedoch im Regelfall nicht erlaubt sein.

Das Beispiel der Meldeevidenz macht dies deutlich. Die Meldepflicht hat den Zweck, von jedem Bürger eine ladungsfähige Adresse zu haben. Diese Adresse ist nach dem Meldegesetz ident mit seinem gewöhnlichen Aufenthalt. Als Kunde eines Versandhauses oder eines sonstigen Unternehmens werde ich aber auch Waren an Adressen bestellen können bzw. dorthin liefern lassen können, wo ich nicht gemeldet bin. Für den Lieferant ist das Melderecht solange belanglos, als die Ware zuverlässig zugestellt werden kann und die Rechnungen bezahlt werden. Ein Abgleich mit den Meldedaten würde hier zusätzliche Fehler bringen. Erst wenn bei Zustellung oder Bezahlung etwas schiefläuft, wird es vielleicht notwendig sein, auf Meldedaten zurückzugreifen. Um das zu können, muss sich der Lieferant jedoch schon vorher über die Identität und die Zahlungsfähigkeit einer Person vergewissert haben.

Im Ergebnis ist die Datenpflege ein mühevolles und personal- und zeitintensives Geschäft, das den eigentlichen Kostenfaktor bei der Verwaltung personenbezogener Daten darstellt.

Wenn der Verantwortliche einem Löschungs- oder Richtigstellungsbegehren des Betroffenen, das heißt seiner Aktualisierungspflicht, 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 DSGVO). Die Höchstrichter werden in Zukunft darüber entscheiden, wie hoch die Strafen tatsächlich sein werden. Weiters hat der Kunde das Recht auf Schadenersatz, sofern ein materieller oder immaterieller Schaden entstanden ist (Art 82 DSGVO).

DATENSCHUTZ-ANFORDERUNGEN FÜR VEREINE GEMÄSS DSGVO

DSGVO Art 4-7, 9, 12-21, 24, 28, 32-37; DSG § 6 Rechtsgrundlage für Datenverarbeitung - Einwilligungserklärung einholen - Rechtsgrundlage für Datenverarbeitung im Verband - Zweckbindungsgrundsatz und Löschungspflicht - Datenschutzrechtliche Informationspflichten - Besondere Kategorien von Daten - Datensicherheit im Verein - Meldepflicht bei Datenschutzverletzungen - Verpflichtung von Mitarbeitern zum Datengeheimnis - Verzeichnis von Verarbeitungstätigkeiten - Vertrag mit Auftragsverarbeiter - Bestellung eines verpflichtenden Datenschutzbeauftragten - Pflicht zur Datenschutzfolgenabschätzung - Rechte der Mitglieder gemäß DSGVO - Dokumentation und Rechenschaftspflicht - Conclusio

Ob auf kultureller Ebene, im sportlichen Bereich, auf Bildungsebene oder auf sozialer Ebene - viele Bürger engagieren sich in Vereinen. Im Zuge der Vereinstätigkeit sind sie immer mit rechtlichen Fragestellungen konfrontiert, beispielsweise mit Fragen des Vereins-, Arbeits-, Sozial- Steuer- sowie Datenschutzrechts. Insbesondere sind datenschutzrechtliche Themen im heutigen IT-Alltag nicht wegzudenken. Auch bei den betroffenen Personen wächst die Sensibilität für Datenschutz.

Für Vereine gilt die Datenschutz-Grundverordnung (DSGVO) und das österreichische Datenschutzgesetz (DSG). Vereine die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von Mitgliederdaten entscheiden, sind deshalb Verantwortliche (Art 4 Z 7 DSGVO). Sofern ein Verein personenbezogene Daten ihrer Mitglieder, Spender, Kunden, ... erhebt, verarbeitet speichert sowie übermittelt, müssen die datenschutzrechtlichen Grundsätze (Art 5 DSGVO beachtet werden. Der Vereinsvorstand als Verantwortlicher ist für die Einhaltung der Datenschutzvorgaben verantwortlich.

Personenbezogene Daten dürfen von Verantwortlichen nur verarbeitet werden, soweit die DSGVO und das DSG oder eine andere rechtliche Bestimmung (Gesetz, Vereinssatzung, ...) dies

zulässt oder die betroffene Person eingewilligt hat. Welche Daten durch den Verein erhoben und verarbeitet werden, hängt von den Vereinszielen ab.

RECHTSGRUNDLAGE FÜR DATENVERARBEITUNG

Vereine dürfen auf Grundlage des Art 6 DSGVO persönliche Daten der Mitglieder erheben, verarbeiten, speichern sowie übermitteln. Als Rechtsgrundlage dient im Verein häufig der Vertrag über die Mitgliedschaft gemeinsam mit der Vereinssatzung. Das Versenden von Newslettern oder die Veröffentlichung personenbezogener Informationen auf der Vereinswebseite setzt zur Erreichung des Vereinszwecks eine Einwilligungserklärung der betroffenen Mitglieder voraus.

In folgenden Fallbeispielen wird veranschaulicht, welche Rechtsgrundlagen bei Datenverarbeitung durch Vereine angewandt werden können:

FALL 1 - NGO (GEMEINNÜTZIGE HILFSORGANISATION), SPENDENFINANZIERT

- Berechtigtes Interesse:
NGOs haben ein überwiegend berechtigtes Interesse bei der Verwaltung von Spenderdaten.

- Rechtliche Verpflichtung:
Weiters verbarbeiten sie Daten ihrer Spender für die Erfüllung einer gesetzlichen Verpflichtung, wie zum Beispiel die steuerrechtliche Spendenabsetzung.

- Einwilligung:
Eine Einwilligung des Spenders ist für die Datenbekanntgabe auf der Vereinswebseite erforderlich, sofern keine vertragliche bzw. satzungsrechtliche Grundlage vorhanden ist.

FALL 2 - FUSSBALLVEREIN

- Erfüllung eines Vertrages:
In der Regel wird zwischen dem Spieler und dem Fußballverein ein zivilrechtlicher Vertrag abgeschlossen. Um den vertraglichen Verpflichtungen gerecht zu werden, kann der Verein für die Dauer der Mitgliedschaft des Spielers sowie seiner Teilnahme am Spielbetrieb die Daten verarbeiten.

- Berechtigtes Interesse:
Ein Fußballverein hat die Verpflichtung gegenüber des österreichischen Fußballbundes (ÖFB) einen geregelten Fußballbetrieb zu gewährleisten. Dies bedeutet beispielsweise, dass die Daten jedes einzelnen, sich im „Kader" befindlichen, Spielers vor Spielbeginn bekannt gegeben werden müssen.

- Einwilligung:
Ein Spieler kann zur Verarbeitung und Veröffentlichung weiterer persönlicher Daten die über die Spielbetriebsrelevanz hinausgehen, einwilligen. Zu denken ist an ein Glückwunschschreiben zur Hochzeit eines Spielers, einschließlich Familienfoto, auf der Vereinswebseite.

FALL 3 - BILDUNGSVEREIN MIT WIRTSCHAFTLICHER TÄTIGKEIT

- Erfüllung eines Vertrages:
Bildungsvereine verarbeiten Kundendaten zur Erfüllung der vertraglichen Verpflichtungen, wie zum Beispiel Kursanmeldung.

- Rechtliche Verpflichtung:
Daneben existieren für Bildungsvereine rechtliche Vorschriften, die unter bestimmten Voraussetzungen eine Verarbeitung ihrer Kundendaten zulassen. Zu denken ist an die steuerrechtliche Aufbewahrungsfrist.

- Einwilligung:
Bei der Veröffentlichung von Kundendaten müssen Bildungsvereine folgendes beachten: Grundsätzlich umfasst die vertragliche Vereinbarung im Bildungsverein nicht die Veröffentlichung von Kundendaten auf der Vereinswebseite. Die Veröffentlichung ist zwar im Interesse des Vereins, aber für die Erfüllung des Vertrags oder der Vereinszwecke nicht notwendig. Daher darf die Veröffentlichung der Daten nur mit ausdrücklicher Einwilligung der betroffenen Kunden erfolgen.

- Berechtigtes Interesse:
Bildungsvereine haben ein berechtigtes Interesse die Daten ihrer Kunden zu verwalten, beispielsweise im Rahmen der Zusendung von neuen Kursangeboten.

FALL 4 - TIERSCHUTZVEREIN

- Berechtigtes Interesse:
Tierschutzvereine haben beispielsweise ein überwiegend berechtigtes Interesse an der Verwaltung von Aktivistendaten.

- Einwilligung:
Vereine dürfen persönliche Daten ihrer Aktivisten nur mit Einwilligung veröffentlichen, sofern keine andere vertragliche bzw. satzungsrechtliche Grundlage vorhanden ist. Organisiert ein Tierschutzverein beispielsweise eine öffentliche Diskussionsveranstaltung, so dürfen Daten ihrer Aktivisten ohne Einwilligung angekündigt werden. Die Datenbekanntgabe durch den Verein erfolgt auf Basis des Vereinszweckes. Damit ist eine zulässige Datenverarbeitung auf Grundlage satzungsrechtlicher Zweckbestimmung gewährleistet.

EINWILLIGUNGSERKLÄRUNG EINHOLEN

Kann sich ein Verein für eine Datenverarbeitung nicht auf eine Rechtsgrundlage stützen, so muss er die Einwilligung einholen. Die Einwilligung darf schriftlich, elektronisch sowie mündlich erfolgen. Die ARGE DATEN empfiehlt Einwilligungen schriftlich mit eigenhändiger Unterschrift der betroffenen Personen einzuholen und aufzubewahren. Die Betroffenen haben jederzeit das Recht die Einwilligung zu widderrufen (Art 7).

Wenn die Einwilligung zusammen mit anderen Erklärungen (beispielsweise Beitrittserklärung) abgegeben wird, ist sie besonders hervorzuheben. Betroffene müssen von sich aus, aktiv eine eindeutige Handlung zur Einwilligung zum Ausdruck bringen.

RECHTSGRUNDLAGE FÜR DATENVERARBEITUNG IM DACHVERBAND

Wenn ein Verein beabsichtigt, die Daten seiner Mitglieder regelmäßig einer Dachorganisation bzw. einem anderen Verein zu übermitteln, sollte dies in der Vereinssatzung geregelt sein. Dadurch wird klargestellt, dass die Übermittlung im Vereinsinteresse erforderlich ist und keine Interessen oder Grundrechte der Vereinsmitglieder überwiegen.

Bei Fehlen einer Satzungsregelung müssen Vereine die Mitglieder über die Übermittlung ihrer Daten an die Dachorganisation bzw. an den anderen Verein und den Übermittlungszweck informieren. Darüber hinaus ist der Verein weiters verpflichtet die Einwilligung der Mitglieder einzuholen. Wenn beide Kriterien erfüllt sind, ist eine datenschutzkonforme Datenübermittlung an dritte Dachorganisationen bzw. Vereine gewährleistet.

Am praktischen Beispiel wird veranschaulicht, welche möglichen Rechtsgrundlagen bei der Datenverarbeitung im Dachverband in Betracht zu ziehen sind: Der Österreichische Fußball-Bund (=ÖFB) als Dachverband ist die gemeinnützige Vereinigung der Fußball-Landesverbände Österreichs (Landesverbände der neun Bundesländer), einschließlich der vielen Fußballvereine. Ein Bundes-Dachverband (ÖFB), der die persönlichen Daten der Mitglieder (Fußballspieler) seiner Mitgliedsvereine (Fußballvereine) verarbeitet, benötigt eine Rechtsgrundlage oder eine Einwilligung der betroffenen Mitglieder. Beispielsweise ist der ÖFB für die Ausstellung von Spielerpässen aller Spieler zuständig ist (§§ 2 iVm 3 Statuten des ÖFB, https://www.oefb.at/OeFB-Satzungen-2017-.pdf?:fi=true&:s=UCKrGXmH&:hp=5141;96484;de).

Grundsätzlich darf der ÖFB die Spielerdaten verarbeiten, sofern eine ausdrückliche Vorschrift (Zweckbestimmung) dies in der Vereinssatzung (Fußballvereine) und auch in den Verbandssatzungen (ÖFB und Fußball-Landesverbände) vorsieht. Eine zulässige Datenverarbeitung wäre nur unter diesen Voraussetzungen gewährleistet. Andernfalls müsste gesondert geprüft werden, ob (a) eine vertragliche Grundlage zwischen dem Fußballverein und dem Spieler vorhanden ist oder (b) ein berechtigtes Interesse des Vereins besteht oder (c) die Einwilligung der Spieler einzuholen ist. Infolgedessen wäre eine datenschutzrechtliche Übermittlungsbefugnis der Fußballvereine begründet.

ZWECKBINDUNGSGRUNDSATZ UND LÖSCHUNGSPFLICHT

Das Erheben und Verarbeiten von Mitgliederdaten ist grundsätzlich nur zur Erfüllung des jeweiligen Zwecks zulässig (Art 6 Abs 1 lit b DSGVO). Eine Datenspeicherung ist nur so lange möglich, wie es für die Erfüllung des Zwecks erforderlich ist. Unter strengen Bestimmungen ist eine darüber hinaus gehende Weiterverarbeitung zulässig. Zu denken ist beispielsweise an die steuerrechtliche Aufbewahrungspflicht der Vereine.

Nach Beendigung der Mitgliedschaft ist eine Weiterarbeitung unzulässig, da die Daten für den Zweck der Verarbeitung nicht mehr erforderlich sind. Insofern besteht gemäß Art 17 DSGVO ein Löschungsanspruch der Mitglieder bei einem Austritt aus dem Verein. Vereine sollten für sämtliche Verarbeitungszwecke entsprechende Löschkonzepte und -fristen festlegen.

Bei der zweckentfremdeten Weiterverarbeitung der Mitgliederdaten (beispielsweise nach Beendigung der Mitgliedschaft) oder einer Erhebung ohne festgelegten Zweck handelt es sich um einen Datenschutzverstoß gemäß Art 83 Abs 5 DSGVO der mit hohen Geldstrafen bedroht wird.

BESONDERE KATEGORIEN VON DATEN

Je nach Vereinszweck werden im Verein Daten erhoben und verarbeitet, die die DSGVO als besonders schützenswert hervorhebt. Zu ihnen zählen beispielsweise Angaben über die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (Art 9 DSGVO). Die Einwilligungserklärung muss klar und deutlich darauf hinweisen, dass die Einwilligung auch besondere Kategorien von Daten umfasst.

DATENSCHUTZRECHTLICHE INFORMATIONSPFLICHTEN

Jeder Verein muss das Transparenzgebot einhalten. Das umfasst die Informierung der Mitglieder zum Zeitpunkt der Erhebung der Daten (Art 12-14 DSGVO).

Folgende Angaben müssen in der Information enthalten sein: Wer welche personenbezogenen Daten zu welchem Zweck und auf welcher Rechtsgrundlage über welchen Zeitraum verarbeitet.

Weiters müssen Angaben über die Betroffenenrechte gemäß Art 15-21 DSGVO, das Bestehen eines Beschwerderechts bei der Datenschutzbehörde und die Pflicht zur Bereitstellung der Daten, enthalten sein. Nähre Informationen über die Informationspflicht der Vereine sind dem Art 13 und 14 DSGVO zu entnehmen.

Vereine sollten gemeinsam mit dem Mitgliedsantrag auch die Datenschutz-Informationen in Schriftform aushändigen. Darüber hinaus ist es auch sinnvoll die Informationen auf der Vereinswebseite zu hinterlegen, wenn sie auch die Möglichkeit zur Online-Mitgliedschaft auf ihrer Vereinswebseite an.

DATENSICHERHEIT IM VEREIN

Vereine sind verpflichtet organisatorische und technische Maßnahmen zu treffen, um eine unrechtmäßige Datenverarbeitung zu vermeiden. Dies impliziert auch Beschränkungen der Zugriffsmöglichkeiten der Vereins-Mitarbeiter. Falls Vereine mit Hilfe von Verteilerlisten eMails an ihre Mitglieder versenden, dann sollte der Blindkopie-Modus (BCC) verwendet werden. Damit ist ein unberechtigtes Empfangen von fremden eMail-Adressen ausgeschlossen. Des Weiteren ist eine Übermittlung von eMails in verschlüsselter Form zu gewährleisten.

MELDEPFLICHT BEI DATENSCHUTZ-VERLETZUNGEN

Kommt es bei der Verarbeitung von Mitgliederdaten zu Sicherheitsvorfällen (beispielsweise Datendiebstahl, Hacking, Fehlver-

sendung, Datenverlust von unverschlüsselten Mitgliederdaten, ...), so bestehen datenschutzrechtliche Meldepflichten (Art 33-34 DSGVO). Die Aufsichtsbehörde ist grundsätzlich über den Sicherheitsvorfall zu unterrichten. Hingegen sind betroffene Personen nur bei hohem Risiko zu informieren.

VERPFLICHTUNG VON MITARBEITERN ZUM DATENGEHEIMNIS

Angestellte Mitarbeiter sowie ehrenamtliche Mitarbeiter im Verein, die mit der Verarbeitung von personenbezogenen Daten betraut sind, sind auf das Datengeheimnis gemäß § 6 DSG zu verpflichten. Die Verpflichtung der Mitarbeiter muss bei Aufnahme der Tätigkeit erfolgen.

VERZEICHNIS VON VERARBEITUNGS-TÄTIGKEITEN

Vereine müssen, wegen der regelmäßigen Verarbeitung der Mitgliederdaten (beispielsweise Mitgliederverwaltung, Lohnabrechnung, Beitragsverwaltung, Veröffentlichung von Mitgliederdaten und -fotos, ...) ein Verzeichnis sämtlicher Verarbeitungstätigkeiten führen (Art 30 DSGVO). Das Verzeichnis soll auch als Grundlage zur Veranschaulichung der Datenverarbeitungsvorgänge dienen. Das Verarbeitungsverzeichnis ist schriftlich oder in elektronischer Form zu führen.

VERTRAG MIT AUFTRAGSVERARBEITER

Viele Vereine nutzen eine externe Adressverwaltung oder einen externen Mailserver. Wenn Vereine die Mitgliedsdaten nicht selbst erfassen und verwalten, dann müssen sie mit Auftragsverarbeitern (in der Regel IT-Unternehmen) einen Vertrag zur Auftragsverarbeitung schließen (Art 28 DSGVO). Der Verein darf nur Auftragsverarbeiter beauftragen, die eine hinreichende Garantie für eine verordnungskonforme Datenverarbeitung gewährleisten kann. Die umfassende Datenschutzverantwortung liegt immer beim Verein.

BESTELLUNG EINES VERPFLICHTENDEN DATENSCHUTZBEAUFTRAGTEN

Vereine müssen sicherstellen, dass für die verpflichtende Bestellung eines Datenschutzbeauftragten eine geeignete Person zur Wahrnehmung der Funktion als Datenschutzbeauftragter im Verein bestimmt wird (Art 37 Abs 1 DSGVO). Wenn keine Gründe gemäß Art 37 Abs 1 für die verpflichtende Bestellung eines Datenschutzbeauftragten vorliegen, dann sollten die Vereine dies mit einer Begründung dokumentieren. In jedem Fall müssen Vereine einen Datenschutzbeauftragten bestellen, wenn die Kerntätigkeit des Vereins eine umfangreiche Verarbeitung besonderer Datenkategorien oder strafrechtlich relevanter Daten ist, wie dies bei weltanschaulichen oder religiösen Beratungsstellen, Parteien, Gewerkschaften, gesellschaftspolitisch engagierte NGOs oder dergleichen der Fall ist.

PFLICHT ZUR DATENSCHUTZ-FOLGENABSCHÄTZUNG

Vereine sind in der Regel verpflichtet eine Datenschutzfolgenabschätzung durchzuführen, wenn eine aufgrund der Art, des Umfangs, der Umstände und Zwecke ein voraussichtlich hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hätte (Art 35-36 DSGVO). Vereine sollten die Eintrittswahrscheinlichkeit und Schwere des möglichen Risikos bewerten. Schließlich sollten geeignete Maßnahmen, Garantien und Verfahren geprüft werden, um bestehende Risiken einzudämmen und verordnungskonform zu verarbeiten. Hier wird eine Zusammenarbeit mit der Datenschutzbehörde verlangt.

RECHTE DER MITGLIEDER GEMÄSS DSGVO

Ferner ist zu berücksichtigen, dass betroffene Mitglieder die ihre Daten bekannt gegeben haben, jederzeit zu Folgendem berechtigt sind (Art 7, 15-21 DSGVO):
- die kostenlose Auskunft darüber, welche Daten von ihnen gespeichert und verarbeitet sind
- die Richtigstellung von falschen oder veralteten Daten
- die Löschung von Daten, die nicht mehr benötigt werden
- die Übertragung der Daten auf einen neuen Verein
- die Erhebung eines Widerspruchs gegen die Datenverarbeitung
- der Widerruf einer Einwilligungserklärung

DOKUMENTATION UND RECHENSCHAFTSPFLICHT

Vereine müssen den Nachweis erbringen, dass die Verarbeitung von Mitgliederdaten nach den in der DSGVO normierten Rechtmäßigkeitsvorschriften erfolgt ist. Dafür wird ein Verarbeitungsverzeichnis geführt, in dem alle Mitgliederdaten dokumentiert werden. Dieses Verarbeitungsverzeichnis soll als eine wesentliche Grundlage zur Umsetzung der Dokumentationspflichten gemäß Art 24 DSGVO dienen.
Ferner erfolgt eine Dokumentation der Einwilligungserklärungen von Mitgliedern, der technischen und organisatorischen Sicherheitsmaßnahmen, der Risikoabschätzung und eine Dokumentation der Vereinbarungen mit Auftragsverarbeitern.

CONCLUSIO

Vereine dürfen persönliche Daten der Mitglieder, Interessenten, Förderer usw. nur für vereinsinterne Zwecke gemäß der Vereinssatzung verarbeiten. Für die Mitgliedsdaten sind Aufbewahrungs- und Löschfristen zu regeln. Sie dürfen Daten nicht an unberechtigte Dritte weitergeben, es sei denn, es liegt eine datenschutzrechtliche Rechtsgrundlage (rechtliche Verpflichtung, Vereinssatzung, Mitgliedschaftsvereinbarung, berechtigtes Interesse sowie Einwilligung) vor.

Die Datensicherheit muss durch technische und organisatorische Maßnahmen sichergestellt sein (aktuelle Betriebssysteme und Anwendungen, Firewall, Virenscanner, passwortgeschützter Zugang, regelmäßiger Backups, Festplattenverschlüsselung, ...). Vereine sind verpflichtet die Mitglieder, deren Daten sie verarbeiten, umfangreich zu informieren. Neben der Informationspflicht haben Vereine umfangreiche Rechte der Mitglieder (Auskunft-, Berichtigung-, Löschungs-, Widerspruchsrecht sowie Recht auf Einschränkung der Verarbeitung und Datenübertragbarkeit) zu beachten und die fristgerechte Erfüllung bei Geltendmachung sicherzustellen.

Jeder Verein muss einen Plan für die Meldung von Datenschutzverletzungen haben. Es ist ein schriftliches Verfahrensverzeichnis über alle Verarbeitungstätigkeiten zu führen. Vereinsmitarbeiter, die mit Mitgliederdaten vertraut sind, müssen eine Verpflichtungserklärung zum Datengeheimnis unterschreiben. Wenn ein Verein Mitgliederdaten nicht allein verarbeitet, sondern Auftragsverarbeiter beauftragt, dann ist ein schriftlicher Vertrag zur Auftragsverarbeitung notwendig. Vereine müssen prüfen, ob eine Bestellung eines Datenschutzbeauftragen erforderlich ist.

VEREINSAUFLÖSUNG - WOHIN MIT DEN DATEN?

DSGVO Art 5-6, 9, 13-14, 17, 82-83
Eine Weitergabe von Mitglieder- oder Mitarbeiterdaten wird nur mit Einwilligung der Betroffenen zulässig sein oder wenn die Nachfolgeorganisation den Vereinszweck in gleichartiger Weise weiterführt. Zur Gleichartigkeit wird unter anderem auch die Gemeinnützigkeit gehören. Bei einem Übergang von einem Verein zu einer kommerziell geführten GmbH wird diese Weiterführung nur in den seltensten Fällen gegeben sein. Für den Fall, dass Datenschutzverletzungen festgestellt werden, können Geldstrafen und Schadenersatzklagen entstehen.

Üblicherweise ist in den Statuten geregelt, wer bei Vereinsauflösung der Begünstigte für das Vereinsvermögen ist. Dies wird meist mit einer allgemeinen Formulierung, wie ‚Dieses Vermögen soll, soweit dies möglich und erlaubt ist, einer Organisation zufallen, die gleiche oder ähnliche Ziele wie dieser Verein verfolgt.' geregelt. Meist entscheidet dann die Generalversammlung wer dieser Begünstigte ist. Oft wird ein Verein nicht schlicht aufgelöst, sondern geht in eine neue Rechtsform über oder fusioniert mit einer anderen Organisation, die Vermögensregelung ergibt sich dann aus dieser Übergangsvereinbarung.

In vielen Fällen verfügen Vereine auch über umfangreiches - personenbezogenes - Datenmaterial, meist Mitgliederdaten, Interessentendaten, eventuell auch Kundendaten, Daten über Mitarbeiter, Referenten, Lieferanten usw.

Diese Daten besitzen zwar oft einen hohen ‚Wert', da sie viele Informationen über Interessenten enthalten, können aber nicht einfach dem Vermögen zugerechnet werden.

Es ist zu beachten, dass jede Organisation nicht einfach personenbezogene Daten besitzt. Alle personenbezogenen Daten, egal in welcher Form und mit welchem Aufwand sie erhoben wurden, dürfen immer nur in Hinblick auf einen bestimmten, rechtmäßigen Zweck verarbeitet werden. Verantwortliche ‚besitzen' keine Daten, sondern sie verfolgen bestimmte Vereins- oder Unternehmenszwecke und im Zuge dieser Zwecke dürfen sie Daten verarbeiten (DSGVO Art 5-6 und Art 9).

Fallen die Zwecke weg, die die ursprüngliche Verarbeitung der Daten rechtfertigten, dann dürfen die Daten nicht mehr verarbeitet werden und sind zu löschen (Art 17 DSGVO).

Wird jedoch im Zuge der Vereinsauflösung mit einer Nachfolgeorganisation die Weiterführung bestimmter Bereiche und Tätigkeiten vereinbart und übernimmt diese Nachfolgeorganisation dazu die Verantwortung, dann dürfen die dazugehörigen Daten, die für den Betrieb dieser Tätigkeiten notwendig sind, ebenfalls an die Nachfolgeorganisation weitergegeben werden. Dies wird etwa bei einem Verein zutreffen, der umfangreiche Schulungs- und Ausbildungstätigkeit durchführte. Die diesbezügliche Interessentendatei wird einer Nachfolgeorganisation die dieselbe Art der Ausbildung anbietet, zu übergeben sein.

Die Details dieser Datenübergabe sind nicht genau geregelt, üblicherweise wird man aber die betroffenen Personen sowohl von der Vereinsauflösung, als auch von der Absicht, ihre Daten zur Weiterführung der bisherigen Tätigkeit an eine neue Organisation zu übergeben, informieren (Art 13-14 DSGVO). Betroffene werden jedenfalls ein Widerspruchsrecht haben und sich gegen diese Datenweitergabe aussprechen können. Es ist daher dafür zu sorgen, dass die Betroffenen zeitgerecht informiert werden und genügend Zeit für einen Widerspruch haben.
Eine Weitergabe jener Daten, die sich auf die Mitgliedschaft des Vereins beziehen, wird nur möglich sein, wenn die Betroffenen dieser Weitergabe ausdrücklich eingewilligt haben. In der Regel bedeutet die Mitgliedschaft zu einem bestimmten Verein auch die Identifikation mit bestimmten Zielen und Ideen. Ob eine Nachfolgeorganisation dieselben Ziele verfolgt, kann nur jedes einzelne Vereinsmitglied selbst entscheiden.

Auch die Daten der Mitarbeiter eines Vereins werden nur mit deren Einwilligung weitergegeben werden dürfen. Die Entscheidung, bei einer neuen Organisation mitzuarbeiten oder sich von dieser Organisation anstellen zu lassen, ist eine persönliche Entscheidung, die jeder einzelne Mitarbeiter treffen muss.

Die Nachfolgeorganisation wird bezüglich der übermittelten Daten zum Verantwortlichen und ist für die Einhaltung der Datenschutzregelungen verantwortlich. Dies bedeutet jedoch nicht, dass diese Daten nunmehr organisationsintern nach Belieben verarbeitet und mit anderen Daten verknüpft werden dürfen. Die Verarbeitung der Daten bleibt auf den ursprünglichen Zweck beschränkt.

Im Übrigen gelten dieselben Regeln auch für Unternehmen die in Konkurs gehen oder fusionieren. Die vielfach kolportierten Unternehmensauflösungen und der ‚Verkauf' des Datenbestandes aus der Konkursmasse kann in vielen Fällen schlicht eine Datenschutzverletzung darstellen.

WELCHE PERSÖNLICHEN DATEN MUSS ICH BEI EINER BEWERBUNG ANGEBEN?

DSGVO Art 5-6, 10, 82-83; GlBG § 26;
In Bewerbungsbögen wird oft die Angabe von persönlichen Daten gefordert. Während die Angabe von Stammdaten und Informationen über Qualifikationen und Fähigkeiten notwendig ist, sind Angaben über Dritte oder auch das Abfragen von ‚soft facts' problematisch und sollten vermieden werden. Bei missbräuchlichem Gebrauch von Bewerberdaten drohen hohe Geldstrafen und Schadenersatzklagen.

BEWERBUNGSBÖGEN GRUNDSÄTZLICH ZULÄSSIG

Viele Unternehmen und Organisationen verlangen von Bewerbern und Bewerberinnen das Ausfüllen von Bewerbungsbogen, um den passenden Kandidaten für eine Stellenausschreibung zu finden (Zweck).

Solche Bewerbungsbogen enthalten in der Regel Angaben zu Stammdaten (Name, evtl. Titel, Adresse, Geburtsdatum, etc.). Daneben sind meistens Eintragungen über die Fähigkeiten des Bewerbers vorgesehen (Ausbildung, frühere bzw. jetzige Berufstätigkeit, Sprachenkenntnisse und ähnliches).

Wer sich bei einem Arbeitgeber um eine Anstellung bewirbt wird in der Regel kein Problem damit haben, solche Daten bekanntzugeben, in aller Regel sind diese auch in den Bewerbungsunterlagen, die vom Bewerber selbst erstellt wurden, enthalten.

ABFRAGE PRIVATER INTERESSEN PROBLEMATISCH

Problematischer ist schon das Abfragen von Daten die nicht die berufliche, sondern vielmehr die private Sphäre eines Bewerbers betreffen. Solche ‚soft facts' sind z.B. Hobbies, Interessen, persönliche Einstellungen, Mitgliedschaften bei Vereinen und Parteien, Krankheitsgeschichten. Oft fehlt dabei jeglicher Zusammenhang zur angestrebten Tätigkeit und es kann auch im Interesse des Bewerbers liegen, solche Informationen für sich zu behalten.

Grundsätzlich darf der Arbeitgeber beispielsweise bei einem Kassierer nach Vorstrafen wegen Vermögensdelikten, bei einem Kraftfahrer nach Straßenverkehrsdelikten und bei einem Erzieher nach Vorstrafen wegen Sexualdelikten fragen.

Hingegen Fragen zu Privatsphäre muss ein Bewerber entweder gar nicht oder kann sie wissentlich falsch beantworten. Aus der Falschbeantwortung einer unzulässigen Frage darf ihm kein Nachteil entstehen.

SONDERFALL VERSICHERUNGSDATENAUSZUG

Aus einem Versicherungsdatenauszug geht hervor, von wann bis wann jemand tatsächlich beschäftigt war. Weiters finden sich auch die genauen Angaben früherer Arbeitgeber. Grundsätzlich ist die Vorlage eines Versicherungsdatenauszuges bei Bewerbungen im Arbeitsmarkt gemäß DSGVO nicht verboten.

Arbeitgeber dürfen in der Regel alle Daten verlangen, die zur Beurteilung der Eignung einer Person erforderlich sind. Darunter können auch Versicherungsdaten eines Bewerbers fallen. Es besteht, aber keinerlei Verpflichtung für Bewerber einen derartigen Versicherungsdatenauszug vorzulegen. Nach herrschender Rechtslage müssen solche Informationen nicht weitergegeben werden und selbst falsche Angaben in diesem Bereich dürfen nicht ohne weiteres dienstrechtliche Konsequenzen haben. Ob diese Vorgehensweise die Bewerber über ihre Aufnahmechancen mindert oder nicht mindert, kann nicht generell beurteilt werden. Bei einer ausreichenden Qualifikation eines Bewerbers, wird der Arbeitgeber sehr wohl andere Kriterien für seine Entscheidungsfindung heranziehen.

ERHEBUNG DER SOZIALVERSICHERUNGSNUMMER FEHLT ZWECK

Vielfach ist die geübte Praxis, dass ein Arbeitgeber auch die Sozialversicherungsnummer eines Bewerbers erhebt. In der Regel wird für das Erheben der Sozialversicherungsnummer bei der Bewerbung der Zweck fehlen. Die Erhebung der Versicherungsnummer ist daher für eine Bewerbung primär nicht bestimmt.

Arbeitgeber dürfen zur Wahrung ihrer berechtigten Interessen Strafregisterauskünfte von Bewerbern verlangen (Art 6 Abs 1 und Art 10 DSGVO). Es ist möglich, dass der Arbeitgeber die Vertrauenswürdigkeit seine Bewerber prüft, wenn eine gefahrengeneigte Tätigkeit, wie zum Beispiel Schaltermitarbeiter bei der Bank, Mitarbeiter im Sicherheitsdienst, geheimhaltungspflichtiger Mitarbeiter eines Forschungsinstitutes, angeboten wird. Die Erhebung der Strafregisterdaten im berechtigten Interesse des Arbeitgebers soll vor Gefahren der Veruntreuung oder zum Schutz der Forschungsarbeit dienen.

Auskünfte einzuholen, ob der Bewerber Einschränkungen physischer oder psychischer Art (Daten nach der Gesundheit) hat, sind grundsätzlich unzulässig. Allerdings ist der Arbeitgeber dann berechtigt Daten nach der Gesundheit eines Bewerbers zu erheben, wenn die Qualität der Tätigkeit beeinflusst sein könnte. In diesem Zusammenhang wäre denkbar, dass eine Bäckerei einen Bewerber fragt, ob ihm Allergien bekannt sind.

DATEN DRITTER DÜRFEN NUR MIT ZUSTIMMUNG BEKANNT GEGEBEN WERDEN

Das Abfragen von Daten Dritter ist problematisch, wie zB Informationen über die Eltern, Ehepartner, Kinder. Für die Verarbeitung von solchen Daten wird in den vielen Fällen der berechtigte Zweck gemäß Art 5 Abs 1 lit. b DSGVO fehlen. Denkbar wäre, dass ein Arbeitgeber nach der beruflichen Qualifikation der Eltern des Bewerbers oder nach einem Nachweis, dass die Eltern des Bewerbers kein Unternehmen betreiben, abfragt, weil er zum Schutz seines Unternehmens nicht daran interessiert ist einen verdeckten Bewerber einzustellen (berechtigtes Interesse). Trotz des berechtigten Interesses des Arbeitgebers ist für die Zulässigkeit der Erhebung der (Eltern)Daten jedenfalls die Einwilligung der Eltern erforderlich.

Gerade bei einer Bewerbung besteht oft ein besonderes Machtgefälle, da Bewerber in der Regel darauf angewiesen sind, möglichst bald eine Stelle zu finden, während ein Unternehmen meist aus mehreren, mehr oder weniger geeigneten Bewerbern, wählen kann. Unternehmen und Organisationen sind daher aufgerufen, in solchen Situationen einen verantwortungsvollen Umgang mit Daten zu pflegen und auf die Erfassung von - in der Regel für die Entscheidung über eine Einstellung völlig irrelevanten - Daten zu verzichten.

Sofern ein Bewerber die notwendigen Daten für die beworbene Stelle veräußert hat und keine Anstellung erhalten hat, können unter Umständen Schadenersatzansprüche geltend gemacht werden (§ 26 Gleichbehandlungsgesetz). Konkrete arbeitsrechtliche Rechtsfolgen können für den Arbeitgeber nur durch nachgewiesene Diskriminierung im Bewerbungsprozess entstehen. Der Anspruch muss binnen sechs Monate ab Ablehnung der Bewerbung geltend gemacht werden.

Für die Klage wegen Diskriminierung ist das Arbeits- und Sozialgericht zuständig. Darüber hinaus, wenn ein Arbeitgeber die Bewerberdaten missbräuchlich erhebt, verarbeitet und speichert drohen konkrete Sanktionen.

DARF EIN UNTERNEHMEN PERSONALISIERTE GESCHENKGUTSCHEINE VERTEILEN?

DSGVO Art 6-7, 9, 14, 17, 82-83
Ausgangslage - Rechtfertigungsgrund oder Einwilligungserklärung - Datenübermittlung an fremde Unternehmen - Einwilligung kann jederzeit widerrufen werden - Geldstrafe und Schadenersatz droht

AUSGANGSLAGE

Ein Arbeitgeber gibt Gutscheine (Einkaufs-, Essens-, Tankgutscheine) an seine Mitarbeiter aus. Diese Gutscheine werden vom Gutscheinprovider ABC ausgestellt. Die Mitarbeiter können diese Gutscheine bei Unternehmen einlösen, die mit dem Unternehmen ABC eine vertragliche Vereinbarung haben („Vertragspartner").

Die Gutscheine sind nicht anonym, sondern enthalten persönliche Daten über die Mitarbeiter (Name, Personalnummer, Arbeitsort etc.). Bei Verwendung des Gutscheins erfährt der „Vertragspartner" persönliche Daten des Mitarbeiters. Eine anonyme Nutzung des Gutscheins ist nicht möglich.

Die Mitarbeiter haben keine Einwilligung zur Verarbeitung ihrer persönlichen Daten durch den Gutscheinprovider ABC gegeben. Der Arbeitgeber hat die Mitarbeiterdaten an den Gutscheinprovider im guten Glauben weitergegeben, den Mitarbeitern „Gutes zu tun".

RECHTFERTIGUNGSGRUND ODER EINWILLIGUNGSERKLÄRUNG

Die Gutscheine enthalten somit personenbezogene Daten gemäß Art 4 DSGVO. Für die Ausstellung der Gutscheine in dieser Form bedarf es daher einer Rechtfertigung gemäß DSGVO.

Ein derartiger Rechtfertigungsgrund könnte - ganz allgemein - eine Rechtsvorschrift, ein Dienstvertrag, ein überwiegendes berechtigtes Interesse des Arbeitgebers (Verantwortlichen) oder eine Einwilligung des Mitarbeiters (Betroffenen) sein (Art 6 DSGVO).

KEINE RECHTLICHE VERPFLICHTUNG DES ARBEITGEBERS

Ein Unternehmen darf Daten von seinen Mitarbeitern aufgrund einer rechtlichen Verpflichtung verarbeiten. Die Steuerbestimmungen verlangen beispielsweise die Aufbewahrung und Weitergabe von Mitarbeiterdaten zur Prüfung der korrekten Verrechnung der Lohnsteuer. Folglich müssen aus steuerlichen Gründen Daten bis zu sieben Jahre aufbewahrt werden. Eine rechtliche Verpflichtung des Unternehmens über das Versehen von Gutscheinen mit persönlichen Angaben der Mitarbeiter besteht jedoch nicht. Dieser Rechtfertigungsgrund kommt daher nicht in Frage.

KEIN BERECHTIGTES INTERESSE DES ARBEITGEBERS

Der Arbeitgeber könnte auch argumentieren, es sei in seinem berechtigten Interesse die Daten der Mitarbeiter weiter zu geben, da er dadurch vom Gutscheinprovider besonders günstige Rabatte erhalten würde.

Dieses Argument ist zwar grundsätzlich richtig, die DSGVO Art 6 beschränkt jedoch das berechtigte Interesse. Es muss sicher gestellt werden, dass die Datenschutzinteressen der Arbeitnehmer nicht beeinträchtigt sind. Es müssen die berechtigten Interessen des Unternehmens stärker sein als die Grundrechte und Grundfreiheiten der Mitarbeiter (Interessensabwägung).

Durch die Angaben des Arbeitnehmers am Gutschein ist ein anonymer Einkauf nicht mehr möglich, persönliche Daten werden „zwangsweise" gegenüber Dritten offen gelegt. Damit besteht jedenfalls ein Eingriff in die Datenschutzinteressen des Arbeitnehmers.

Das berechtigte - wirtschaftliche - Interesse des Unternehmens für das Versehen der Gutscheine mit persönlichen Daten der Mitarbeiter, wird in diesem Fall gegenüber den Datenschutzinteressen der Arbeitnehmer kein ausreichender Rechtfertigungsgrund sein. Die Interessensabwegung wird zu ungunsten des Arbeitgebers ausfallen.

VEREINBARUNG IM ZUGE DER ANSTELLUNG THEORETISCH MÖGLICH

Zulässig ist auch die Verarbeitung von Mitarbeiterdaten, die für die Erfüllung eines Dienstvertrages erforderlich sind. Zu denken ist an die besondere Bestimmungen bei der Nutzung eines Firmenwagens zu Privatzewecken und ähnliches. Die Rechte und Pflichten von Arbeitgeber und Arbeitnehmer sind in diesem Fall vertraglich vereinbart und können nur gemeinsam geändert werden.

So könnte im Dienstvertrag auch vereinbart werden, dass Geschenk-Gutscheine oder sonstige freiwillige Sozialleistungen nur dann gewährt werden, wenn der Arbeitnehmer mit der Weitergabe bestimmter, im Dienstvertrag genau angeführter Daten an einen Gutscheinprovider einverstanden ist.
Einer der Gründe für diese Vorgangsweise könnten besonders günstige Konditionen für den Einkauf der Gutscheine sein. Sozusagen Datenhandel im Gegengeschäft zu Gutscheinrabatten.

Der ARGE DATEN sind jedoch keinerlei derartige Dienstverträge bekannt und es bestehen auch berechtigte Zweifel, ob ein derartiger Dienstvertragspassus vor dem Arbeitsgericht hält.

EINWILLIGUNG DES MITARBEITERS ERFORDERLICH

Um Mitarbeiterdaten auf Gutscheinen aufzudrucken ist somit eine Einwilligung des Mitarbeiters einzuholen.

Die Einwilligung nach der DSGVO muss gemäß Art. 7 DSGVO für jede Verarbeitung, der sie als Rechtfertigung dienen soll, ausdrücklich erklärt werden. Es muss auch angegeben werden welche Daten zu welchen Zweck an wen verarbeitet und übermittelt werden. Pauschaleinwilligungen á la „das Unternehmen darf Daten weiter geben" sind unzulässig.

Der Arbeitgeber muss den Mitarbeitern über den Zweck der Verarbeitung, über die konkret zu verarbeitenden Daten und ihre jederzeitige Widerrufbarkeit aufklären. Diese Aufklärung muss den Bestimmungen des DSGVO Art. 14 entsprechen.

EINWILLIGUNG KANN JEDERZEIT WIDERRUFEN WERDEN

Hat der Arbeitgeber eine gültige Einwilligung erwirkt, dann muss er mit dem jederzeitigen Widerruf einer Einwilligung rechnen. Derartige Widerrufe können unbegründet und jederzeit erfolgen. Mit dem Widerruf verbunden ist das Recht auf Löschung gemäß Art 17 DSGVO.

ZUSTIMMUNG IST NICHT ERSETZBAR

Es ist ein weit verbreiteter Irrglaube, dass die verpflichtende persönliche Zustimmung durch eine Betriebsvereinbarung ersetz werden könnte. Die DSGVO verlangt eindeutig und klar eine persönliche Zustimmung jedes Einzelnen. Im Rahmen einer Betriebsvereinabrung könnte jedoch Höhe der Gutscheine, Ausgabemodus, Gültigkeitsdauer oder dergleichen geregelt werden.

SONDERFALL UNTERNEHMENSINTERNE GUTSCHEINE

Einen Sonderfall stellen unternehmensinterne Gutscheine dar. Ein Arbeitgeber gibt seinen Mitarbeitern in den Geschäften seines Unternehmens einen bestimmten Rabatt oder stellt Einkaufsgutscheine aus.

In diesem Fall werden keine Daten an andere Verarbeiter als dem Arbeitgeber weiter gegeben. Hier kann der Arbeitgeber erfolgreich argumentieren, dass der Gutschein zur Verhinderung des Missbrauchs personalisiert wird und daher ein überwiegendes berechtigtes Interesse besteht. Die Datenschutzinteressen des Arbeitnehmers werden in diesem Fall in den Hintergrund treten, da das Unternehmen nur wenige zusätzliche Informationen erhält.

Dieser Sonderfall kann aber nicht bei besonders schutzwürdigen Daten in Anspruch genommen werden. So dürften Spitäler - ohne Zustimmung der Mitarbeiter - keine Behandlungs-Gutscheine ausstellen und dadurch Einblick in den gesundheitlichen Status der Mitarbeiter erhalten.

ENTSORGUNG ALTER PERSONALUNTERLAGEN

DSGVO Art 17, 32, 82-83; DSG § 1; ABGB §§ 16, 1328a; StGG Art 9-10a UGB §§ 77-78, 87
Alle Mitarbeiterunterlagen unterliegen dem Datenschutz - Nicht mehr benötigte Daten sind zu löschen - Billige Entsorgung illegal - Vielfältige Strafbestimmungen betroffen

ALLE MITARBEITERUNTERLAGEN UNTERLIEGEN DEM DATENSCHUTZ

Die ARGE DATEN wird immer wieder mit Datenschutzfragen zu Mitarbeiterunterlagen konfrontiert. Schon mehrmals wurde auf die beschränkte Verwendungsmöglichkeit von Bewerbungsunterlagen hingewiesen. So ist etwa eine längerdauernde Evidenzhaltung einer Bewerbung oder gar die Weitergabe an andere Unternehmen, auch innerhalb eines Konzerns an die Einwilligung des Bewerbers gebunden.

Den meisten Unternehmen ist auch bewusst, dass Personalakte als besonders schützenswert angesehen werden und daher sorgfältig aufzubewahren sind. Doch wie schaut es mit Zeitaufzeichnungen, Projektblättern oder Spesenabrechnungen aus? Insbesondere dann, wenn die Abrechnungen abgeschlossen sind und schon mehrere Jahre zurückliegen. Was könnte man schon aus den Daten herauslesen?

Grundsätzlich ist anzumerken, dass vom DSGVO nicht nur elektronisch verarbeitete Daten erfasst sind, sondern auch Akten, manuelle Aufzeichnungen und Listen. Alle Unterlagen, unabhängig vom Speichermedium fallen daher unter den Datenschutz.

Die DSGVO kennt auch keine Unterscheidung zwischen wichtigen und unwichtigen persönlichen Daten. Grundsätzlich fallen alle Daten unter die Geheimhaltung, auch eine „Verjährung" von persönlichen Daten ist nicht vorgesehen. Solange die Daten existieren ist der Verantwortliche zur Datensicherheit nach dem Stand der Technik verpflichtet.

NICHT MEHR BENÖTIGTE DATEN SIND ZU LÖSCHEN

Umgekehrt besteht jedoch die Verpflichtung, nicht mehr benötigte Daten gemäß Art 17 DSGVO zu löschen, für Ausdrucke, aber auch für handschriftliche Aufzeichnungen bedeutet dies, dass sie unrekonstruierbar zu vernichten sind.

Personalabteilungen und alle anderen Unternehmensabteilungen die personenbezogene Aufzeichnungen haben, haben daher einerseits die Verpflichtung regelmäßig zu prüfen, welche Unterlagen nicht mehr notwendig und daher zu vernichten sind. Eine derartige Prüfung wird sinnvollerweise im Rahmen der jährlichen Inventur stattfinden.

Weiters muss die Vernichtung mit geeigneten Mitteln erfolgen. Das bloße Deponieren im Müllcontainer oder das Vergessen der Unterlagen „irgendwo" wäre unzulässig.

BILLIGE ENTSORGUNG ILLEGAL

Sicher unzulässig wäre die Praxis, wie sie im Zusammenhang mit einem bekannten Personalbereitsteller bekannt wurde, gleich kistenweise 3-4 Jahre alte Personalunterlagen, Bewerbungsbögen, Lebensläufe, Zeitaufzeichnungen und Kundenabrechnungen inkl. der gesamten Korrespondenz, auf öffentlichen Parkplätzen zu deponieren. Und so kann auch jeder Interessierte lesen, welche Personen bekannte Mineralölfirmen, Elektrokonzerne, Ministerien oder Banken „angemietet" hatten.

Doch wie lautete die Datenschutzerklärung gleich? „Wir treffen alle erforderlichen Vorkehrungen zum Schutz Ihrer Daten um zufällige oder vorsätzliche Manipulationen zu verhindern. Die Sicherheitsmaßnahmen entsprechen stets dem Stand der technischen Entwicklung und werden dieser auch laufend angepasst."

Und so kann jeder der will über Stellenbewerber folgende Kommentare lesen „sehr suspekt!", „schwitzt", „lange Haare", „rundes Gesicht", ... Selbstverständlich inklusive Name und Telefonnummer. Eben Stand der Technik.

VIELFÄLTIGE STRAFBESTIMMUNGEN BETROFFEN

Neben der Verletzung der Datensicherheitsbestimmungen (Art 82-83) können eine Reihe weiterer Bestimmungen verletzt sein. Unter anderem die Verletzung der Privatsphäre (§1328a und §16 ABGB), das Grundrecht auf Geheimhaltung (Art 9, 10 u. 10a StGG, §1 DSG). Auch Verletzungen des Urheberrechts (§77, §78, §87 Abs 2 UrhG) wären denkbar, etwa wenn Mitarbeiterfotos unzulässig veröffentlicht werden.

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 finanziell 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

GILT INNERHALB DER FAMILIE DATENSCHUTZ?

DSGVO Art 6, 77; DSG § 1, 4
Datenschutz innerhalb der Familie in Zusammenhang mit Behörden - DSGVO auch gegenüber nahen Angehörigen anwendbar - keine Anwendung der DSGVO innerhalb rein familiärer Angelegenheiten

BEHÖRDEN GEBEN DATEN AN FAMILIENANGEHÖRIGE WEITER

Im Rahmen eines Studienbeihilfeverfahrens wird der antragstellenden Studentin nicht nur mitgeteilt, dass sie keinen Anspruch auf Studienbeihilfe hat, weil der Erziehungsberechtigte mehr verdient als die Beihilfegrenze vorsieht, sondern auch das genaue Jahreseinkommen des Erziehungsberechtigten. Es ergibt sich damit die grundsätzliche Frage, ob Daten zwischen Familienangehörigen auch dem Datenschutz unterliegen.

Grundsätzlich unterscheidet die Datenschutz-Grundverordnung (DSGVO) in seiner Wirkung nicht zwischen verschiedenen Verwandtschaftsformen oder Personenbeziehungen. Datenschutz ist ein subjektives Recht, das jeder Person, auch Minderjährigen zukommt. Die einzigen zulässigen Einschränkungen sind allgemein im § 1 Datenschutzgesetz (DSG) umschrieben und ergeben sich aus der Abwägung der Geheimhaltungsinteressen gegenüber anderen Rechten und Interessen.

Kinder und Jugendliche dürfen ab dem vollendeten 14. Lebensjahr eine datenschutzrechtliche Einwilligungserklärung abgeben (§ 4 Abs 4 DSG). Bei Minderjährigen wird etwa das Erziehungswohl und die Entwicklung der Persönlichkeit, aber auch die Entscheidungen des Erziehungsberechtigten in vielen - aber nicht allen - Fällen, Vorrang gegenüber Datenschutzinteressen haben. Ebenso wird das alltägliche Leben im Familienverband, in einer gemeinsamen Wohnung usw. in vielen Fällen zu einem Zurücktreten des Rechts auf Privatsphäre und Datenschutzes führen. Die Bereiche sind nicht abschließend geregelt und es macht auch keinen Sinn hier Detailregelungen für jeden Sachverhalt zu finden. Das Familienrecht, das Eherecht, das Allgemeine Bürgerliche Gesetzbuch, werden im Zweifelsfall für die Abgrenzung zwischen Privatsphäre der einzelnen Ehepartner und Familienmitglieder heranzuziehen sein.

Völlig anders stellt sich jedoch die Situation dar, wenn es um die Entscheidungen von Behörden geht. Diese werden ausschließlich auf Basis von bestehenden Gesetzen Daten verarbeiten und weitergeben können und im Zweifelsfall wird die vertrauliche Behandlung von Informationen Vorrang haben (Art 6 DSGVO). Im konkreten Fall ist die Kenntnis über die tatsächliche Höhe des Einkommens für den Studienbeihilfenbescheid völlig irrelevant und wird daher ohne Einwilligung des Betroffenen nicht weitergegeben werden dürfen. Angemessen wäre bloß die Feststellung gewesen, dass die Beihilfe nicht gewährt wird, weil das Einkommen des Erziehungsberechtigten über der Beihilfengrenze liegt. Nun könnte argumentiert werden, dass das tatsächliche Einkommen wesentlich für die Bemessung allfälliger Unterhalts- oder Ausbildungszahlungen ist. Trotzdem hätte die Studienbeihilfenbehörde eine Datenschutzverletzung begangen. Es liegt nämlich nicht in der Kompetenz der Studienbeihilfenbehörde sich Gedanken über Unterhaltszahlungen zu machen. Dafür sind Gerichte - falls sich die Beteiligten nicht einigen können - zuständig. Der in seinen Persönlichkeitsrechten verletzte Erziehungsberechtigte kann daher Beschwerde bei der Datenschutzbehörde (DSB) erheben (Art 77 DSGVO).

KEINE ANWENDUNG DER DSGVO INNERHALB REIN FAMILIÄRER ANGELEGENHEITEN

Für familiäre Angelegenheiten hat die DSGVO eine weitreichende Ausnahme festgelegt. Die sogenannte House-Hold-Exeption des Art. 2 DSGVO nimmt alle familiären Tätigkeiten von der Anwendung der DSGVO aus.

Damit können Eltern Kinder überwachen, Fotos machen, deren Smartphones abhören, eMails lesen oder auch persönliche Aufzeichnungen ausspionieren. In keinem Fall findet die DSGVO Anwendung. Für Kinder gilt das im übrigen auch gegenüber ihren Eltern, ebenso bei Ehepartnern oder sonstigen familären Konstellationen.

KEIN FREIBRIEF ZUR TOTALEN ÜBERWACHUNG

Trotzdem darf nicht unbeschränkt überwacht werden. Das Eindringen in die Privatsphäre ist neben der DSGVO durch eine Vielzahl anderer Bestimmungen geregelt. Die wichtigsten sind die EMRK Art. 8, die EU-Charta Art. 7, Urheberrechtsgesetz §§ 77,78 oder ABGB § 1328a, um nur einige wichtige zu nennen.

So wird das beliebte Kinder-Tracking nur mit dem Kindeswohl begründbar sein. Wenn es tatsächlich im Interesse des Kindes ist „überwacht" zu werden, zB bei einem Ausflug in gefährliches Gelände, ist Tracking erlaubt. In allen anderen Fällen riskieren die Eltern Verletzungen der Privatsphäre, der Menschenrechte oder des Urheberrechts, Geltung des Datenschutzes hin oder her.

SIND ALLE AUFNAHMEN GEMÄSS DSGVO BILDAUFNAHMEN?

DSGVO Art 5-6, 30, 82, 83 DSG §§ 12-13
Nicht jede Installation einer Kamera bedeutet auch Überwachung - Rein technische Aufnahmen fallen nicht unter Bildaufnahmen im Sinne des Datenschutzgesetz - Identifizierung und Zweck sind maßgeblich

Bildaufnahmen gemäß Datenschutz-Grundverordnung (DSGVO) und Datenschutz-Gesetz (DSG) liegt dann vor, wenn Aufnahmen in identifizierender Absicht erfolgen, also zum Ziel haben im Ereignisfall (meist rechtswidriges Verhalten) eine Person zu identifizieren.

Rein technische Aufnahmen fallen nicht unter Bildaufnahmen gemäß § 12 DSG. Beispielsweise installiert der Betreiber einer Autowaschstraße eine Videoüberwachungsanlage. Der Zweck der Bildaufnahme gemäß Art 5 Abs 1 lit b und 6 Abs 1 lit f DSGVO ist die Kontrolle der ein- und ausfahrenden Autos auf schon vorhandene Schäden, um beweisen zu können, dass beanstandete Schäden nicht beim Waschvorgang entstanden sind.

Beschränkt sich die Bildaufnahme ausschließlich auf die Waschanlage zum Zeitpunkt des Betriebes als technische Aufnahme, zu dem üblicherweise niemand im Auto sitzt oder sonstwie erfasst wird, handelt es sich um keine Bildaufnahme gemäß Datenschutzrecht.

Werden jedoch Aufzeichnungen geführt um etwa spätere Reklamationen zu verhindern oder sonstwie das gereinigte KFZ und damit auch den Besitzer zu identifizieren (etwa über das KFZ-Kennzeichen), dann wäre sehr wohl auch eine Bildverarbeitung gegeben.

Zu bedenken ist, dass jeder Verwendungsvorgang von Videoüberwachungssystemen gemäß Art 30 DSGVO zu protokollieren ist. Nicht erforderlich ist dies lediglich bei einer Echtzeitüberwachung. Hingegen ist die Kennzeichnungspflicht gemäß Art 13 DSG ausnahmslos für jeden Verarbeitungsvorgang zwingend.

Eine verordnungswidrige Bildverarbeitung kann gemäß Art 83 Abs 5 DSGVO mit einer Geldstrafe von bis zu 20 Millionen Euro bzw. vier Prozent des weltweiten Umsatzes durch die Datenschutzbehörde verhängt werden. Neben der Geldstrafe enthält der Art 82 Abs 1 DSGVO eine Anspruchsgrundlage zum Ersatz materieller und immaterieller Schäden für Datenschutzverletzungen. Die Zivilgerichte sind für Schadenersatzklagen zuständig.

IST DAS GEBURTSDATUM AUF BRIEFZUSENDUNGEN ZULÄSSIG?

DSGVO Art 4-6, 82, 83
Informationen über die Schutzwürdigkeit des Geburtsdatums auf Poststücken.

Grundsätzlich ist das Geburtsdatum gemäß Art 4 Datenschutzgrundverordnung (DSGVO) ein besonders schutzwürdiges Faktum. Das Anbringen auf einem Briefumschlag oder sonst wie auf der Außenseite eines Poststückes ist ein Eingriff in die Privatsphäre.

Dies gilt - in allgemeiner Form - auch für jede andere persönliche Information, die über die Angabe des Namens und der notwendigen Adress-Merkmale für eine sichere Zustellung hinausgehen (Art 5, 6 DSGVO).

Nach Entscheidungen der Datenschutzbehörde K210.174/0016-DSK/2013 bzw. K121.337/00007-DSK/2007 ist die Angabe des Geburtsdatums dann zulässig, wenn es zur sicheren Identifikation persönlich adressierter Schreiben dient (z.B. Rsa-Briefe), ansonsten ist die Notwendigkeit nicht gegeben. Rsa-Schreiben müssen persönlich zugestellt werden. Mit Hilfe des Geburtsdatums und eines Personalausweises kann der Zusteller (Briefträger) feststellen, wer der tatsächlich Empfangsberechtigte ist. (alte Rechtslage bis 24.05.2018)

Weiters ist das Geburtsdatum auf der Postsendung des Verteidigungsministeriums, die bloß eine Soldateninfobroschüre enthält, nicht zulässig (K210.380/001-DSK/2001), auf einer Ladung der Polizei jedoch schon (K120.888/001-DSK/2004). (alte Rechtslage bis 24.05.2018)

Zusätze zur Adresse, die nicht der näheren Bestimmung des Adressaten dienen, sind ein Verstoß gegen die DSGVO. Bericht der Datenschutzbehörde 1993 im Sinne der alten Rechtslage bis 24.05.2018: „Die DSB hat in einem Fall erkannt, dass ein Strafbezirksgericht gegen das Datenschutzgesetz verstoßen habe, weil es eine Urkunde mit dem Codewort ‚BedV1' auf dem Kuvert zustellen ließ. ‚BedV1' ist mittels Formbuches in Strafsachen entschlüsselbar (‚bedingte Verurteilung'). Die Anführung des Codes auf zuzustellenden Schriftstücken ist in keiner Rechtsvorschrift vorgesehen. Dieser Code war ohne Bedeutung für das Gerichtsverfahren und nicht vom Richter angeordnet." (alte Rechtslage bis 24.05.2018)

Eine verordnungswidrige Datenverarbeitung kann gemäß Art 83 Abs 5 DSGVO mit einer Geldstrafe von bis zu 20 Mio. Euro bzw. 4% des weltweiten Umsatzes durch die Datenschutzbehörde bestraft werden. Neben der Geldstrafe enthält der Art 82 Abs 1 DSGVO eine Anspruchsgrundlage zum Ersatz materieller und immaterieller Schäden für Datenschutzverletzungen. Die Zivilgerichte sind für Schadenersatzklagen zuständig.

DATENSCHUTZSTENOGRAMM 2018/19

14. FEBRUAR 2019
EUGH-Entscheidung (C-345/17): Filmaufnahmen von einer Privatperson in einer lettischen Polizeistelle wurden auf Youtube hochgeladen - Berufung auf den Begriff der „Haushaltsausnahme“ ist nicht möglich bzw. kann die Veräffentlichung nicht als journalistische Tätigkeit bezeichnet werden
http://curia.europa.eu/juris/document/document.jsf?text=&docid=210766&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=7804641

12. FEBRUAR 2019
EDPB veröffentlicht Leitlinien zu Verhaltenskodex und Überwachungsstelle betreffend der Verordnung 2016/679 (DSGVO)
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf

23. JÄNNER 2019
EDPB veröffentlicht die angenommenen Leitlinien 1/2018 für Zertifizierung und identifying certification in Bezug auf Artikel 42 und 43 der Datenschutz-Grundverordnung
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_1_2018_certification_en_0.pdf

21. JÄNNER 2019
Die französische Datenschutz-Behörde CNIL verhängt eine Strafe gegen Google von 50 Millionen Euro.

14. JÄNNER 2019
EU-Kommission erkennt Japans Datenschutz als gleichwertig an
http://europa.eu/rapid/press-release_IP-18-5433_en.htm

4. DEZEMBER 2018
EDPB veröffentlicht Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der Datenschutz-Grundverordnung (2016/679)
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2018-12-04-guidelines_4_2018_accreditation_de.pdf

16. NOVEMBER 2018
EDPB veröffentlicht Leitlinien 3/2018 zum territorialen Anwendungsbereich der Datenschutz-Grundverordnung (Artikel 3)
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf

9. NOVEMBER 2018
Verordnung der Verarbeitungen die verpflichtend eine Datenschutz-Folgenabschätzung durchführen müssen.
https://www.ris.bka.gv.at/eli/bgbl/II/2018/278/20181109
http://ftp.freenet.at/privacy/ds-at/dsfa-v.pdf

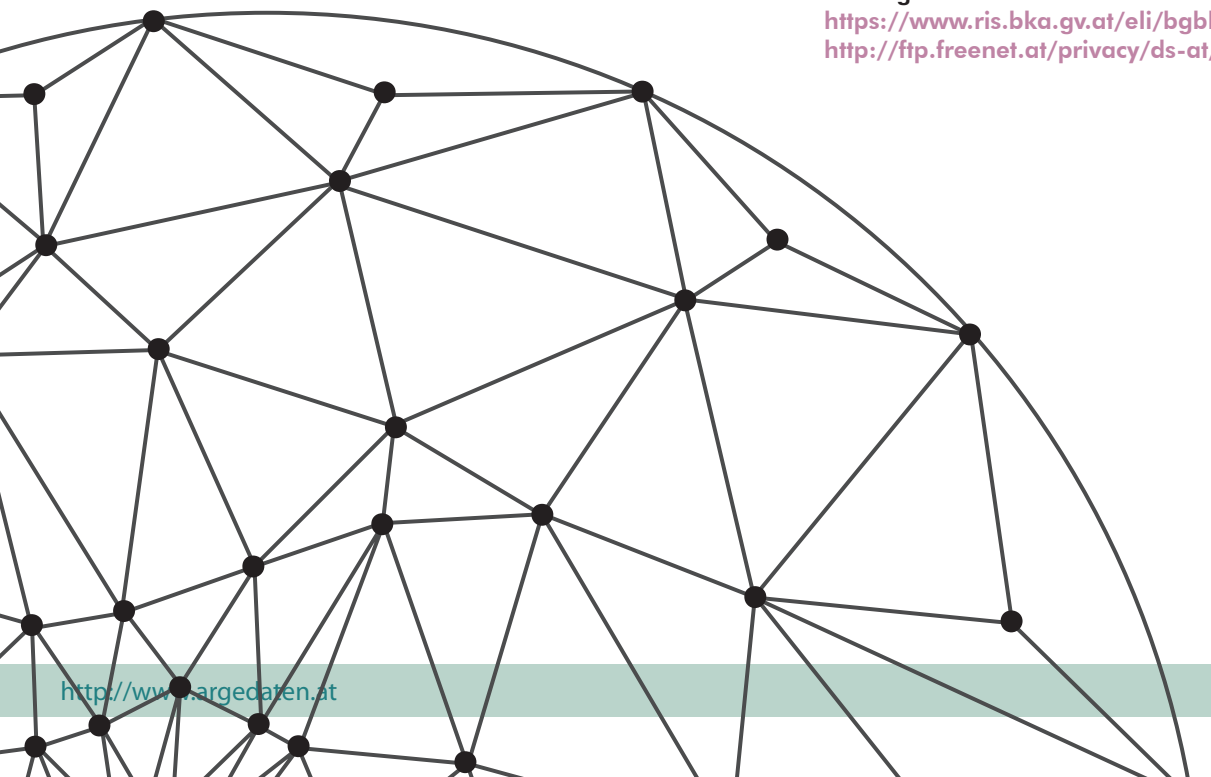
13 SEPTEMBER 2018
EGMR verkündet Urteil im Fall BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM
https://hudoc.echr.coe.int/

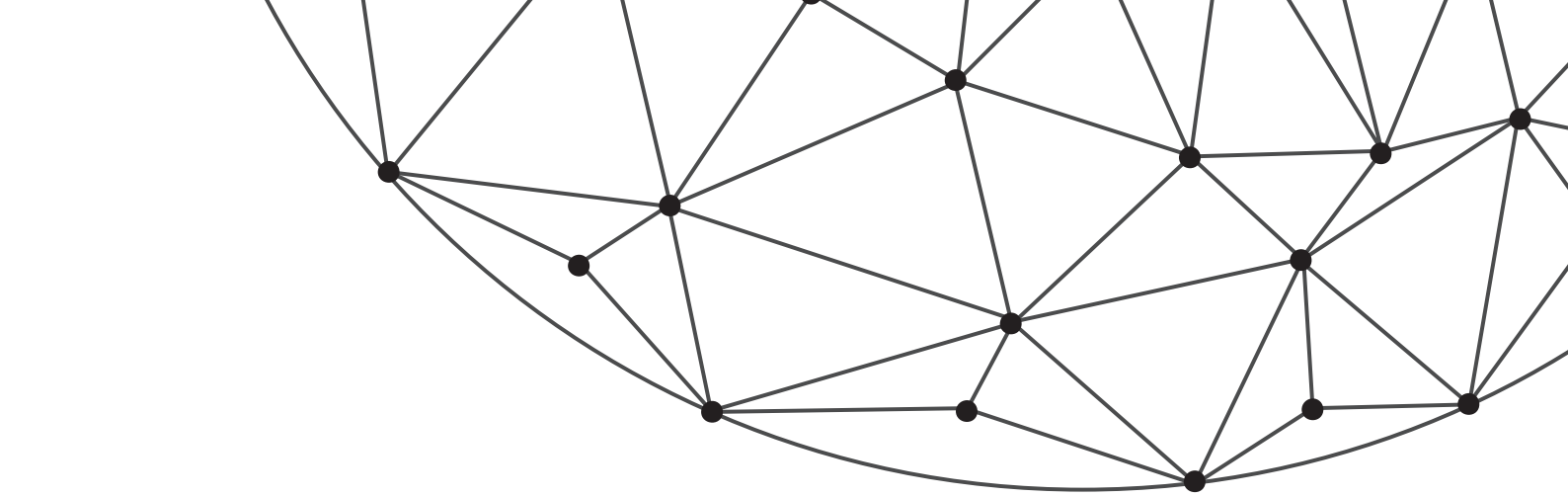
10. JULI 2018
EUGH-Urteil (C-25/17): personenbezogene Daten, welche bei Verkündigungstätigkeiten der Zeugen Jehovas beim Gang von Haus zu Haus anfallen, unterliegen auch den Regelungen der DSGVO
http://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=7804641

14. JUNI 2018
Das zweite Datenschutzanpassungspaket wird im Bundesgesetzblatt veröffentlicht. 100 Gesetze sind betroffen.
https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2018_I_37

25. MAI 2018
Ab diesem Tag MUSS die Datenschutz-Grundverordnung in allen EU-Mitgliedstaaten unmittelbar angewendet werden. DSG (neu) enthält Bestimmungen zur Durchführung der Datenschutz-Grundverordnung in Österreich.
http://ftp.freenet.at/privacy/ds-at/dsg2018-aktuell.pdf

25. MAI 2018
Datenschutzbehörde veröffentlicht Verordnung mit Datenverarbeitungen, welche keine Datenschutz-Folgenabschätzung benötigen
https://www.ris.bka.gv.at/eli/bgbl/II/2018/108/20180525
http://ftp.freenet.at/privacy/ds-at/dsfa-av.pdf





25. MAI 2018
EDPB veröffentlicht Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Datenschutz-Grundverordnung
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_de.pdf

25. MAI 2018
Der europäische Datenschutz-Ausschuss EDPB („European Data Protection Board") konstituiert sich.
https://edpb.europa.eu/our-work-tools/agenda/2018_en

17. MAI 2018
Das erste Datenschutzanpassungspaket wird im Bundesgesetzblatt veröffentlicht. 125 Gesetze sind betroffen.
https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2018_I_32

16. MAI 2018
Nationalrat beschließt zahllose weitere Datenschutz-Anpassungen, in Summe sind .
https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00108/index.shtml
https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00068/index.shtml

16. MAI 2018
Das Datenschutz-Anpassungsgesetz 2018 - Wissenschaft und Forschung - WFDSAG 2018 mit zum Teil sehr problematischen Zugriffsmöglichkeiten auf ELGA-Daten und andere Gesundheitsdaten wird im Bundesgesetzblatt publiziert. Datenschutzbestimmungen in 17 Gesetzen sind betroffen.
https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2018_I_31

15. MAI 2018
Zeitgleich werden zwei getrennte Änderungen des Datenschutzgesetzes (DSG) im Bundesgesetzblatt publiziert. Neben Beschränkungen der Betroffenenrechte soll auf diesen Weg auch auf die Tätigkeit der Datenschutzbehörde Einfluss genommen werden.
https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2018_I_24
https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2018_I_23

26. APRIL 2018
Sicherheitspaket wird im Nationalrat beschlossen. Neben Änderungen der Datenschutzbestimmungen werden auch Bundestrojaner, Vorratsdatenspeicherung „light" (sogenannte Anlassdatenspeicherung) und erweiterte Ermittlungsbefugnisse der Polizei beschlossen
https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00015/index.shtml

20. APRIL 2018
In geradezu Orwellscher Newspeak beschließt Nationalrat ein „Datenschutz-Deregulierungsgesetz", dass unter anderem die Auskunfts- und Geheimhaltungsrechte der Betroffenen beschränkt und der Datenschutzbehörde vorschreibt, keine Strafen zu verhängen. Weiters sollen private Unternehmen, sofern sie im öffentlichen Auftrag handeln, straffrei bleiben. Nutznießer dürften unter anderem KFZ-Werkstätten sein, die § 57a KFG-Überprüfung machen. Alle diese „Sonderregeln" widersprechen der DSGVO und sind wohl EU-widrig.
https://www.parlament.gv.at/PAKT/VHG/XXVI/BNR/BNR_00027/index.shtml

30. MÄRZ 2018
Bundeskanzleramt + 10 Ministerien haben Entwürfe zur Umstellung ihrer Ressort-Gesetze auf die Anforderungen der DSGVO veröffentlicht.
https://www.parlament.gv.at/PAKT/MESN/

21. MÄRZ 2018
Datenschutzbehörde veröffentlicht Verordnungsentwurf zu jenen Verarbeitungen, die KEINER Datenschutz-Folgenabschätzung gemäß Art. 35 bedürfen.

7. MÄRZ 2018
Österreichs Ministerien beginnen mit der Umstellung ihrer Gesetze auf die Anforderungen der DSGVO, das Bundesministerium für Inneres (BMI) veröffentlicht als erstes einen Entwurf.

13. FEBRUAR 2018
Art. 29 - EU-Datenschutzgruppe veröffentlicht Leitlinien zu Profiling und automatisierte Einzelentscheidung (Automated individual decision-making and Profiling)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

13. FEBRUAR 2018
Art. 29 - EU-Datenschutzgruppe veröffentlicht Leitlinien zu Verständigung bei Datenschutzverletzungen (Guidelines on Personal data breach notification)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

24. JÄNNER 2018
EU-Kommission veröffentlicht „Leitfaden zur unmittelbaren Anwendbarkeit der Datenschutz-Grundverordnung"
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52018DC0043&from=DE

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

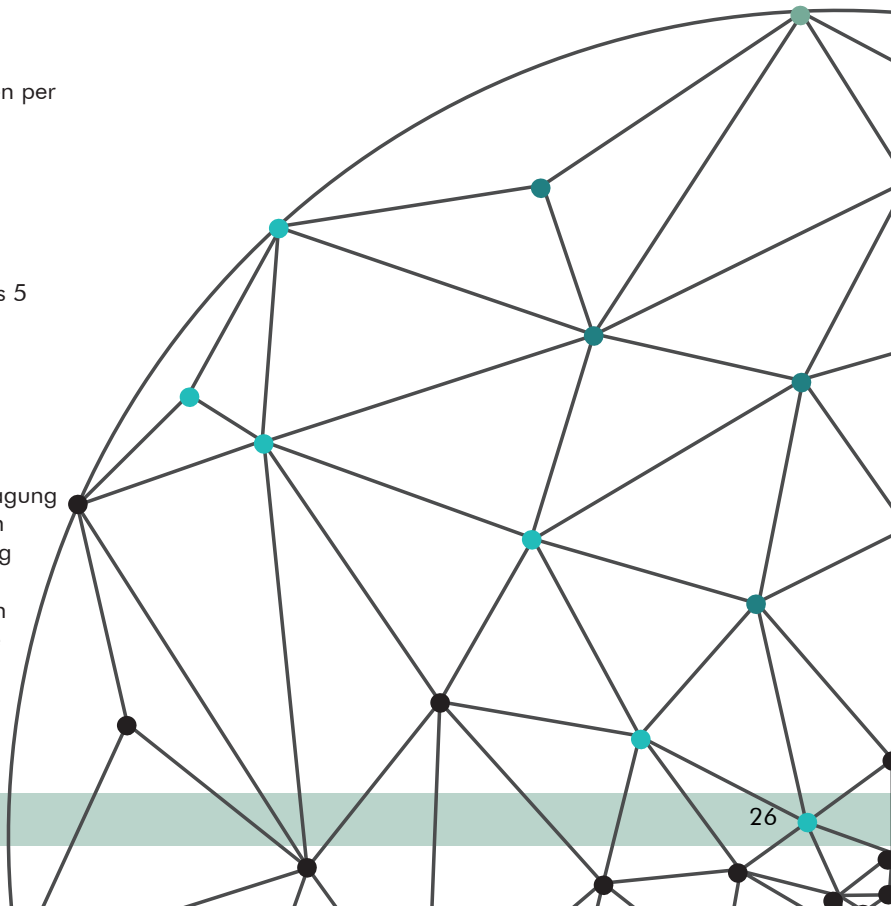
Geeignet für kleine und mittlere Unternehmen mit geringer Zahl an personenbezogenen Datensätzen und geringe Zahl von Verarbeitungen (max 3)

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)

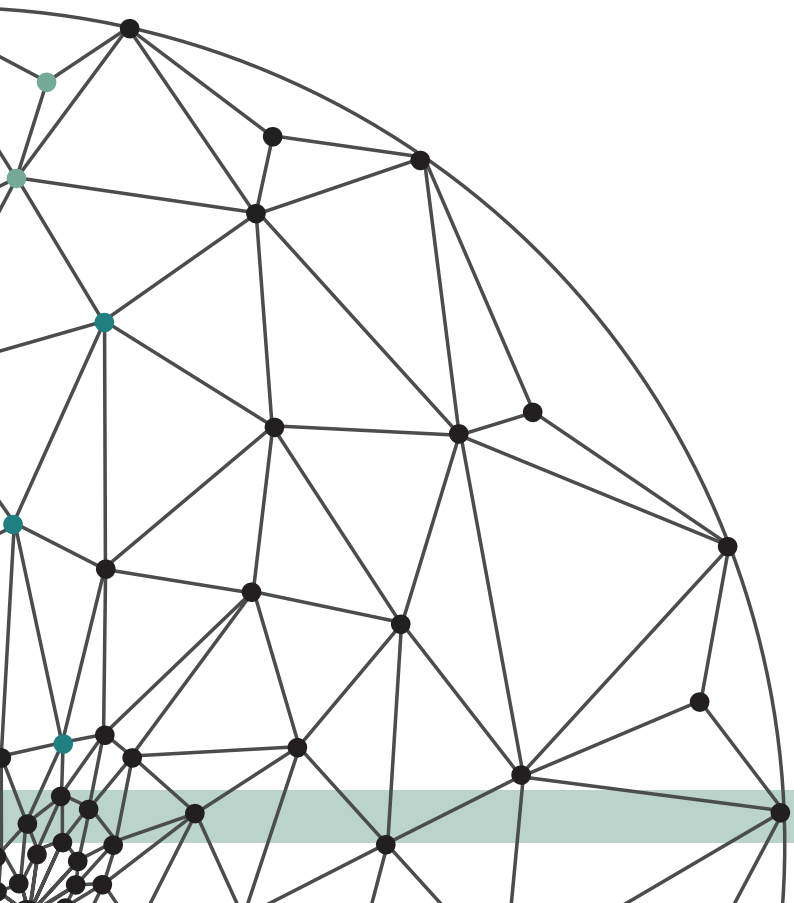


EXTERNER DATENSCHUTZBEAUFTRAGTER - FULL

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

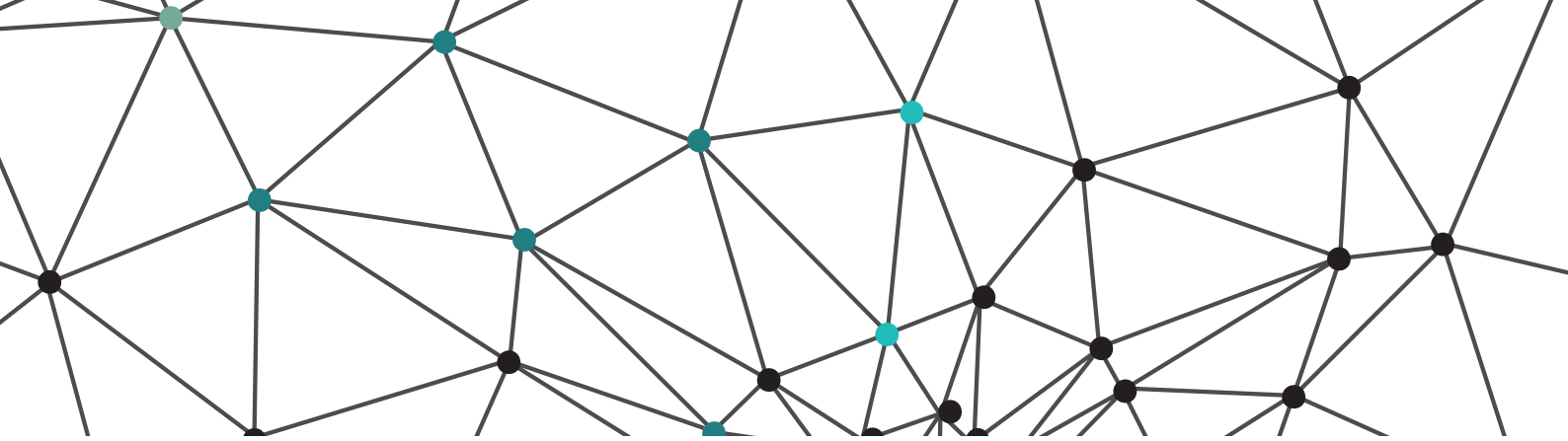
Servicebetrieb zur Abwicklung von Bestellungen und Verrechnung:
e-commerce monitoring GmbH, HG Wien FN 224536 a
http://www.e-monitoring.at

Bildnachweis:
S. 8, 13, 19, 22 siehe Quelle www.pixabay.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 ist Ihnen Frau Indra 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.