PRIVACY AUSTRIA TÄTIGKEITSBERICHT 2019/20

ARGE DATEN

http://www.argedaten.at/

EDITORIAL

Der Jahresbericht der ARGE DATEN soll unseren Lesern die Datenschutzentwicklung des abgelaufenen Jahres, die Tätigkeit der ARGE DATEN und die Zukunft des Grundrechts auf Datenschutz näher bringen.

Heuer ist alles anders. Der Großteil des Berichts folgt dieser Tradition und eigentlich hatte ich geplant auf die Entwicklungen nach Einführung der Datenschutz-Grund-Verordnung (DSGVO) einzugehen. Allem voran mit der im Oktober 2019 verhängten Rekordstrafe von 18 Millionen Euro gegen die Post AG.

Ein Betrag der auf Grund der Bestimmungen der DSGVO durchaus gerechtfertigt ist, trotzdem jedoch den „falschen" trifft.

EUROPAS WERBEMARKT WIRD PERSONALISIERT

Was war die Ausgangslage? Der europäische Werbemarkt ist etwa 110 Milliarden Euro schwer. Vor 7 Jahren (2018) betrug er etwa 90 Mrd Euro, ist also um etwa 25% gewachsen. Eine florierende Wirtschaft und kein Thema eines Datenschutz-Jahresberichts?

Nur wer alle Zeichen der Zeit ignoriert. In diesen 7 Jahren kam es - praktisch unbemerkt - zu einem höchst dramatischen Wandel der Werbestruktur. Machte 2011 die Werbung bei Zeitungen und Zeitschriften etwa 33% des Kuchens aus, waren es 2018 nur mehr die Hälfte, etwa 16%. Gleichzeitig stieg der Anteil der Online-Werbung von 21% (2011) auf das Doppelte, nämlich 42% (2018).

In anderen Worten, die - datenschutzrechtlich gesehen - anonymisierte Inseratenwerbung wurde durch personalisierte Online-Werbung abgelöst. Interessanterweise konnten alle anderen Werbeformen (TV, Radio, Kino, Outdoor) ihre Umsätze über diesen Zeitraum weitgehend halten.

Die absoluten Zahlen machen die Sachlage noch dramatischer: aus 30 Mrd Euro Umsatz im Print-Bereich (2011) wurden 18 Mrd Euro im Jahr 2018, bei gleichzeitig gestiegenen Produktionskosten für die Printmedien. Aus 19 Mrd Euro Umsatz (2011) für die Online-Werbung wurden 48 Mrd Euro im Jahr 2018, bei gleichzeitig sinkenden Internetkosten.

BIGDATA-PRODUKT ONLINE-USER

Auf diese Situation versuchte die Post AG zu reagieren und am personalisierten Werbemarkt mitzunaschen, mit höchst fragwürdigen Ideen. So sollten aus verfügbarem Datenmaterial politische bzw. weltanschauliche Präferenzen der ÖsterreicherInnen ermittelt werden, aus den Postnachsendeaufträgen weitere Interessen abgeleitet werden. BigData auf österreichisch eben. Ob die Post AG damit wahnsinnig viel Geld verdiente darf bezweifelt werden, die Profis dieser Branche sitzen in den USA.

Dazu eine abschließende Zahl: die 42 Mrd Euro Online-Werbung in EU-Europa sind höchst ungleich verteilt. Google allein hatte sich 2018 davon 21 Mrd Euro geschnappt. Also die Hälfte der gesamten Online-Werbung oder mehr als alle Printmedien der EU zusammen an Inseraten lukrieren konnten.

Dahinter liegt Facebook - schon mit Abstand - bei 7 Mrd Euro. Das sind, gemäß den eigenen Angaben von Facebook, durchschnittlich 22 Euro pro EU-MAU. Als MAU bezeichnet Facebook jeden „Monthly Active User", also jeden Facebook-Account, der zumindest einmal im Monat aufgerufen wird.

Wer noch immer nicht begreift, dass der Sozial Media - Nutzer das Produkt und nicht der Kunde ist, dem ist nicht zu helfen.

MIT CORONA IST ALLES ANDERS

Doch in der Fertigstellung des Berichts erwischte uns die Corona-Pandemie und es ist mir ein Bedürfnis besonders auf die grundrechtlichen Konsequenzen einzugehen.

Damit ist nicht die unsägliche Stopp-Corona-App des Roten Kreuzes gemeint, die nicht praxistauglich ist und sicher keinen Beitrag zur Krisenbewältigung leisten wird. Da hilft auch der Sicherheits-Persilschein wohlwollender Techniker nichts. Die ARGE DATEN hatte dazu ausführlich berichtet.

Diese Stopp-Corona-App kann bestenfalls als moderne Amulettform gesehen werden, ähnlich wie Hufeisen, Kleeblätter und gekreuzte Finger. „Nützt's nichts, schadet's nicht" könnte man meinen.

Diesen Spruch gibt es jedoch im Zeitalter der globalen Vernetzung nicht. Jeder Nutzer der Stopp-Corona-App musste sie aus dem Apple/iOS- oder Google/Android-Store downloaden. Apple- und Google haben damit eine weitere Information über ihr BigData-Produkt Online-User, vormals: Mensch. Auch wenn Google/Apple in die App nicht hinein schauen können, erhalten sie einen perfekten Überblick über die Bewegungen des Nutzers und mit welchen anderen iOS- oder Android-Usern er Kontakt hatte. Und zwar unabhängig davon, ob der andere auch die Stopp-Corona-App hatte oder nicht.

Praxistauglich ist die Stopp-Corona-App nicht, aber dafür eine weitere BigData-Quelle für Google und Co.

GRUNDRECHTE VOR BEWÄHRUNGSPROBE

Datenschutz ist ein wichtiges Grundrecht, Gesundheit ebenfalls, Erwerbsfreiheit, Meinungsfreiheit, Versammlungsfreiheit, Religionsfreiheit und das Recht auf Familienleben sind einige weitere Grundrechte.

Keines dieser Grundrechte gilt absolut, es ist immer eine Balance zu finden. Offene und demokratische Gesellschaften setzen dabei auf das Individuum und vernunftorientiertes Verhalten, Eingriffe werden auf ein Minimum reduziert.

Dieses Prinzip hat Österreich seit März 2020 verlassen. Standen am Anfang der Pandemie Zögerlichkeit, Ignorieren und „Durchtauchen", folgten danach ausladende, undifferenzierte Maßnahmen, bemüht die Ängste in der Bevölkerung zu verstärken, statt Probleme zu lösen. Eine ganze Gesellschaft wurde in den Stillstand geschickt, euphemistisch als „Home-Office", „Home-Learning" und „Home-Shopping" verbrämt.

Selbst das regierungsseitig behauptete Primat des Grundrechts auf Gesundheit wurde über Bord geworfen. März/April 2020 erlebte Österreich auch in der Gesundheitsversorgung abseits von Corona einen beispiellosen Stillstand.

Österreich wird noch Jahre an den sozialen, gesundheitlichen und wirtschaftlichen Folgen leiden.

NEIN ZUM CORON-ARIER-AUSWEIS

Die Corona-Situation lockt auch zahllose Politiker und Berater, bis weit in die Regierung, hervor, denen Grundrechte nur ein lästiges Anhängsel sind. Mittlerweile werden ernsthaft Pläne für einen Coron-Arier-Ausweis gewälzt.

Personen mit überstandener COVID-19-Erkrankung sollen sich als „immun" ausweisen dürfen und damit keinen Beschränkungen unterliegen. Es ist noch nicht lange her, als ein totalitäres Regime einen vergleichbaren Ausweis für den Zugang zum öffentlichen Leben einführte.

Wie unsäglich dumm diese Idee ist mögen wenige Zahlen zeigen. Österreich hatte (Stand Mai 2020) etwa 15.000 „genesene" Personen. Das sind 0,2% der Gesamtbevölkerung. Eine „Elite" mit der kein Produktionsbetrieb, keine kritische Infrastruktur und auch kein Tourismus betreibbar wäre.

Hinzu kommt, dass die Fehlerquote bei den Coronatests bei etwa 15% liegt. Selbst unter dieser „immunen" Gruppe könnten bis zu 2.000 Personen sein, die NICHT immun sind.

Abgesehen davon wäre ein derartiger Corona-Arier-Ausweis auch ein fürchterliches Signal an alle bisher gesunden Menschen. Ihr umsichtiges Verhalten würde mit Diskriminierung bestraft.

DIGITALE STEINZEIT IN EUROPA

Gnadenlos bloßgestellt hat die Corona-Situation auch die informationstechnischen Schwächen von Österreich und von EU-Europa.

„Home-Office", „Home-Learning" und „Home-Shopping" werden mit Smartphone, Outlook, Facebook, WhatsApp, Amazon, Skype, Zoom, Teams, GotoMeeting, Teamviewer, Google-Drive und OneDrive bestritten. Viele halten das für modern.

Faktum ist, dass weder das österreichische Bildungssystem, noch die österreichischen KMUs auf digitales Arbeiten vorbereitet waren. Die zitierten Produkte sind durchwegs US-amerikanischer Herkunft, niemand in Europa weiß, was mit den dort gesammelten Daten tatsächlich passiert.

Darüber hinaus sind diese Verfahren nicht in betriebliche Prozesse, in die Ausbildungsstrukturen integrierbar. Ihre Verwendung verursacht zahllose Sicherheitslücken und Doppelgleisigkeiten, effizientes Arbeiten wird zur Illusion.

Noch Ende 2018 bestritt der famose Bildungsminister Fassmann die Verwendung von US-Produkten im Schulunterricht (wir berichteten darüber). Jetzt in Corona-Zeiten lobt er erbendiese Verwendung durch Lehrer und Schüler als Digitalisierungs-Fortschritt.

Kaum eine Behörde, eine Bildungseinrichtung oder ein Unternehmen hat in Österreich eine geeignete Informationsinfrastruktur für digitales Arbeiten. Bastellösungen und Improvisieren mit US-Produkten sind vorherrschend.

Dadurch überrascht auch das häufigste Corona-Betrugszenarium nicht. Es befinden sich zahllose Emails mit gefaktem Absender (meist irgendeine Behörde oder ein Vorgesetzter) im Umlauf, in denen entweder Identifikationsdaten oder Kontodaten verlangt werden oder gleich Firmenzahlungen auf Fremdkonten verlangt werden. Das sind - formal - völlig korrekte eMails, oft sogar von bekannten Virenscannern als schadsoftwarefrei gekennzeichnet. Keine Firewall, kein Virenscanner kann derartige eMails filtern. Die Angriffe könnten leicht abgewehrt werden, wenn jedes echte Email elektronisch signiert wäre. Die flächendeckende Einführung einer Signatur-Infrastruktur würde schlagartig 90% der Betrugsversuche verhindern.

Mehr Datenleitungen, mehr Tablets, mehr Smartphones sind zu wenig. Ohne geeignete Arbeitskonzepte bleiben sie informationstechnischer Schrott. Österreich und die EU entwickeln sich zu einer Konsumentengesellschaft, die Geräte aus China und Dienste aus den USA verwendet.

Mittelfristig droht allen Branchen das Schicksal der europäischen Werbeindustrie, der europäischen Printmedien, der Dolmetscher, ... Selbst Beratungsberufe, wie Rechtsanwälte, Ärzte oder Steuerberater stehen mittlerweile im Visier von Google und Co. Möglich wird das durch das unermüdliche Füttern dieser Unternehmen mit Informationen, egal ob datenschutzrelevant oder nicht.

Vergleicht man die weltweit größten 60 Internetfirmen, beträgt die Marktkapitalisierung der US-Unternehmen etwa 4.500 Mrd USD, danach folgen - mit Respektabstand - die asiatischen Firmen mit etwa 1.200 Mrd USD. Europa ist weit abgeschlagen mit 250 Mrd USD. Selbst Afrika kommt mittlerweile den Europäern mit 100 Mrd USD nahe.

Österreich muss endlich das Informationszeitalter ernst nehmen, sonst bleiben uns nur noch geschützte Werkstätten und Tätigkeiten als Museumswärter oder Gärtner. Und selbst diese Jobs sind in Zeiten der coronabedingten Reisebeschränkungen nicht mehr krisensicher.

Bleiben Sie virenfrei

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

AUFREGER DES JAHRES

18 MIO STRAFE FÜR DIE ÖSTERREICHISCHE POST AG

Für große Aufregung im vergangenen Jahr sorgte die Verarbeitung und Weitergabe von persönlichen Daten samt ermittelter Parteienaffinität durch die Österreichische Post AG. Im Prüfungsverfahren durch die Datenschutzbehörde stellte sich heraus, dass die Post AG persönliche Daten im großen Stil verarbeitete und diese anschließend an Unternehmen und politische Parteien verkaufte.

In einer eigenen Datenbank, getrennt von allgemeinen Kundendaten, wurden Datensätze mit marketingrelevanten Informationen wie Adresse, Name, Geschlecht, Erwerbstätigkeit, aber auch die Parteienaffinität gespeichert. Man kann sich berechtigt die Frage stellen, wie die Zusammenhänge mit einer Parteizugehörigkeit geschaffen wurden.

Die Datenermittlung erfolgte mittels eigenentwickelter Berechnungssysteme. Dafür wurden Ergebnisse aus Umfragen, Hochrechnungen, Statistiken und Wahlergebnissen mit anderen personenbezogenen Daten wie Adresse, Name und Geschlecht abgeglichen. Die Richtigkeit der Einschätzung lag allerdings bei 50 Prozent. Im Umkehrschluss wurde der Hälfte der Betroffenen falsche Parteienaffinität unterstellt. Das könnte ein Verstoß nach DSGVO bedeuten, weil die verarbeiteten personenbezogenen Daten sachlich falsch waren. Ein weiterer Verstoß könnte die Verarbeitung von Daten besonderer Kategorie ohne triftigen Grund sein, darunter fällt auch politische Meinung. Das natürlich unter der Annahme, dass die Parteienaffinität personenbezogene Information ist.

Die ausgewerteten Daten konnten von verschiedenen Unternehmen gemietet, geleast oder gekauft werden. Bei Miete konnten die Daten nur einmal verwendet werden, bei Leasing war die Nutzung ein Jahr lang uneingeschränkt möglich und beim Kauf gab es keine zeitliche Begrenzung.

Auch politische Parteien haben davon gebrauch gemacht. Dabei haben die Parteien ohnehin Zugriff auf die Adressen von wahlberechtigten ÖsterreicherInnen. Nun ist es naheliegend, dass mit ausgewerteten Daten gezielte Werbung besser betrieben werden kann.

Die österreichische Datenschutzbehörde verhängte eine stolze Strafe in Höhe von 18 Millionen Euro. Das ist die höchste Strafe, die die unabhängige Behörde bis jetzt verhängt hat. Bis jetzt gab es in der DSGVO-Geschichte EU-weit drei ebenbürtige Strafen.

Die britische Datenschutzbehörde verhängte umgerechnet 205 Millionen Euro Strafe für British Airways. Durch eine Sicherheitslücke im Online-Buchungssystem konnte beim Cyberangriff auf persönliche Daten (Name, Adresse, Kreditkartennumer samt CVV Code, usw) von 500.000 Kunden zugegriffen werden. Dabei handelte es sich zwar um keinen bewussten Datenschutzmissbrauch, die IT-Sicherheit gehört aber zum Datenschutz, so die Datenschutzbehörde.

Die zweithöchste Strafe in Höhe von umgerechnet 110 Millionen Euro wurde für die Hotelkette Marriott durch die englische Information Commissioner Office (ICO) ausgesprochen. Es handelte sich um einen ähnlichen Fall wie bei British Airways. Die Computersysteme der Hotelkette wurden zu wenig geschützt.

Der Konzernriese Google gestaltete seine Datenschutzbestimmungen nicht transparent genug und konnte dazu keine wirksame Einwilligung in die Verarbeitung der Daten für Werbezwecken nachweisen. Dafür kassierte Google 50 Millionen Strafe von der französischen Datenschutzbehörde CNIL.

Die Entscheidung der österreichischen Datenschutzbehörde ist noch nicht rechtskräftig. Die Österreichische Post AG hat Berufung beim Bundesverwaltungsgericht eingereicht. Vor der Rechtskraft gilt die Unschuldsvermutung.

WIE ENTSTEHEN SO HOHE STRAFEN?

Die DSGVO sieht drastische Strafen vor, die einen abschreckenden Charakter haben sollen. Die Höhe der Strafe hängt von Faktoren wie Art, Schwere, Dauer, Vorsatz oder Fahrlässigkeit, Anzahl geschädigter Personen usw. ab und kann bis 20 Millionen oder 4 Prozent des weltweiten Jahresumsatzes bei einem Unternehmen reichen, je nachdem welcher Betrag höher ist.

Art. 83 DSGVO zählt mögliche Pflichtverletzungen auf, diese Aufzählung ist demonstrativ und soll der Verdeutlichung dienen, ist aber nicht abschließend.

Lediglich zwei Verpflichtungen fallen nicht in die Kategorie des Art. 83 und sind nach DSGVO nicht mit der Strafe bedroht. Dabei handelt es sich um Verbot strafrechtlich relevante Daten zu verarbeiten (Art. 10) und Pflicht zur Implementierung technischer und organisatorischer Compliance-Maßnahmen (Art. 24). Den Mitgliedstaaten wurde die Regelung für den Fall einer Verletzung freigelassen.

Die Strafe für die Österreichische Post AG mit einem Jahresumsatz vom knapp 2 Milliarden (Geschäftsjahr 2018) hätte deutlich höher ausfallen können. Wenn höchste Ermessungsgrundlage von 4 Prozent herangezogen worden wäre, würde die Strafe bei circa 80 Millionen liegen.

AUSBILDUNGSREIHE „BETRIEBLICHER DATENSCHUTZBEAUFTRAGTER“

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.

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 Datenschutzfolgeabschätzung statt sinnleerer Formularwirtschaft.

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.

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.

CERTIFIED BY AUSTRIAN STANDARDS


Zertifikat

Die ARGE DATEN -
Österreichische Gesellschaft für Datenschutz
bestätigt, dass Herr

Max Mustermann

die Veranstaltungsreihe

Betrieblicher Datenschutzbeauftragter

erfolgreich abgeschlossen hat.

Modul 1 Datenschutz Grundlagen | Modul 2 Datenverwendung im Unternehmen | Modul 3 Datenschutz und IT-Sicherheit | Modul 4 Datenschutz EU-Grundverordnung | Modul 5 Datenschutz praktische Umsetzung

Wien, am 8.11.2017

DI Erwin Sulzgruber
Schriftführer

ARGE DATEN

Dr. Hans

MIT ZERTIFIKAT ZUM „BETRIEBLICHEN DATENSCHUTZ-BEAUFTRAGTEN"

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.

TÄTIGKEITSBERICHT ARGE DATEN 2018/19

Beispiele aus der Beratungspraxis der ARGE DATEN

- **Bonität:** Löschung der negativen Einträge gegenüber den Wirtschaftsauskunftsdiensten
- **Gesundheit:** Zulässigkeit der Verarbeitung von gesundheitlichen Daten
- **Briefverkehr:** Weitergabe von personenbezogenen Daten an Dritte
- **KFZ:** Pickerlüberprüfung und die Speicherdauer veralteter Gutachten
- **Behörden:** Vorgehensweise beim Auskunftsbegehren
- **Bank:** Selbstauskunft über gespeicherte Daten, Widerrufsrecht
- **Privatleben:** Recht auf Widerspruch bei Smart Metern
- **Behörden:** Speicherdauer von biometrischen Daten
- **Konsum:** Kundenkarten bei großen Konzernen und Datenerfassung
- **Gesundheit:** Austritt und Löschung der ELGA-Daten. zeitliche Wirksamkeit des Austritts
- **DSGVO:** Informationen zum Recht auf Löschung, negative Auskunft über gespeicherte Daten
- **Personenverkehr:** Zulässigkeit der Erfassung von Daten zu berechtigten Zwecken / Scannen der Fahrausweise
- **Statistik:** Richtige Vorgehensweise bei Mikrozensuserhebungen
- **Gesundheit:** Erfordernisse an Formulare zur Einsicht in Patientendaten
- **Berufsleben:** Qualifizierte elektronische Signatur und datenschutzrechtlicher Zusammenhang

Öffentlichkeitsarbeit, Informationsdienst

Im Rahmen unseres Mediendienstes und der Öffentlichkeitsarbeit erreichen wir regelmäßig circa 5000 datenschutzinteressierte Personen und konnten zahlreiche Medienanfragen zum Datenschutz beantworten.

Veranstaltungen, InHouse-Schulungen

2019/20 nahmen 125 Personen an unserer Jahresdatenschutztagung zu spannenden datenschutzrechtlichen Themen teil. Diese Veranstaltung erfreut sich großer Beliebtheit, seit Beginn haben schon über 950 Personen daran teilgenommen.

AUTOMATISIERTE KENNZEICHENERFASSUNG BEI PARKGARAGE

Im Bescheid (DSB-D123.652/0001/2019) vom 4. Juli 2019 beschäftigte sich die Datenschutzbehörde mit der Frage der Zulässigkeit einer automatisierten Kennzeichenerfassung bei einer Parkgarage zwecks Abrechnung der Garagennutzung.

Laut Sachverhalt handelte es sich bei der Beschwerdegegenerin um die Betreiberin eines größeren Einkaufszentrums, welches die Nutzung einer Parkgarage erlaubt. Bei der Einfahrt in die Garage wurde das Kfz-Kennzeichen des Beschwerdeführers von einer Kamera automatisch erfasst. Der Beschwerdeführer behauptete eine Verletzung im Recht auf Geheimhaltung sowie einen Verstoß gegen das Koppelungsverbot, da die Benutzung der Garage nur dann möglich ist, wenn man die automatisierte Erfassung des Kennzeichens dulde. Die Beschwerdegegnerin stützte die KFZ-Erfassung auf berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO.

KENNZEICHENERFASSUNG ÜBLICH

Die Datenschutzbehörde hielt zunächst fest, dass neben dem Kennzeichen weitere personenbezogene Daten verarbeitet werden, wie Zeitpunkt und Ort, an dem sich der Beschwerdeführer als Halter und Fahrer aufgehalten habe. Des Weiteren wurde die Informations- und Kennzeichnungspflichten offenbar nicht ordnungsgemäß umgesetzt, da der Verarbeitungszweck, nämlich die Erfassung des Kennzeichens zwecks Abrechnung der Garagennutzung, nicht auf dem Schild vor der Einfahrt angeführt wurde.

Das ist nach Ansicht der Datenschutzbehörde nicht weiter problematisch, zwar ist im Rahmen einer Interessenabwägung auch auf die vernünftige Erwartungshaltung abzustellen, allerdings ist die automatisierte Kennzeichenerfassung zwecks Abrechnung der Geragennutzung nicht unüblich (Bescheid der DSB vom 18. März 2019 GZ DSB-D196.007/0005-DSB/2019, mit welchem Verhaltensregeln gemäß Art. 40 Abs. 5 DSGVO betreffend Garagen- und Parkplatzbetriebe in Österreich inhaltlich genehmigt wurden). Um den datenschutzrechtlichen Anforderungen gerecht zu werden, hat der Beschwerdegegner geeignete technische und organisatorische Maßnahmen getroffen (u.a. sofortige Löschung der personenbezogenen Daten nach Abwicklung der Abrechnung).

ÜBERWIEGENDES INTERESSE BEI KURZNUTZUNGSVERTRÄGEN

Die Datenschutzbehörde ist zum Entschluss gekommen, dass die Interessen der Raschheit und Effizienz bei der Abwicklung von Kurznutzungsverträgen überwiegen. Die Beschwerdegegnerin hat die Daten für keinen anderen Zweck, als für die Abwicklung der Abrechnung verarbeitet und somit auch keine Berechtigten Interessen des Beschwerdeführers berührt.

Auf einen Verstoß gegen das in Art. 7 Abs. 4 DSGVO normierte „Koppelungsverbot" war nicht einzugehen, da die Beschwerdegegnerin die Verarbeitung nicht auf eine Einwilligung gemäß Art. 6 Abs. 1 lit.a DSGVO gestützt hat.

Eine Verletzung der Informationspflichten nach Art. 13 DSGVO war nicht Gegenstand des Verfahrens. Die Beschwerde wurde daher abgewiesen.

SCHULNOTEN SIND PERSONENBEZOGENE INFORMATION

Im Bescheid (DSB-D123.594/0003-DSB/2019) vom 2. August 2019 hatte sich die Datenschutzbehörde mit der Frage befasst, ob die Mitteilung der Schulnoten an die Klassensprecherin das Recht auf Geheimhaltung verletzt. Der Lehrer teilte die genaue Notenzusammenstellung der Beschwerdeführerin mit, um die Unstimmigkeiten in der Klasse zu beseitigen.

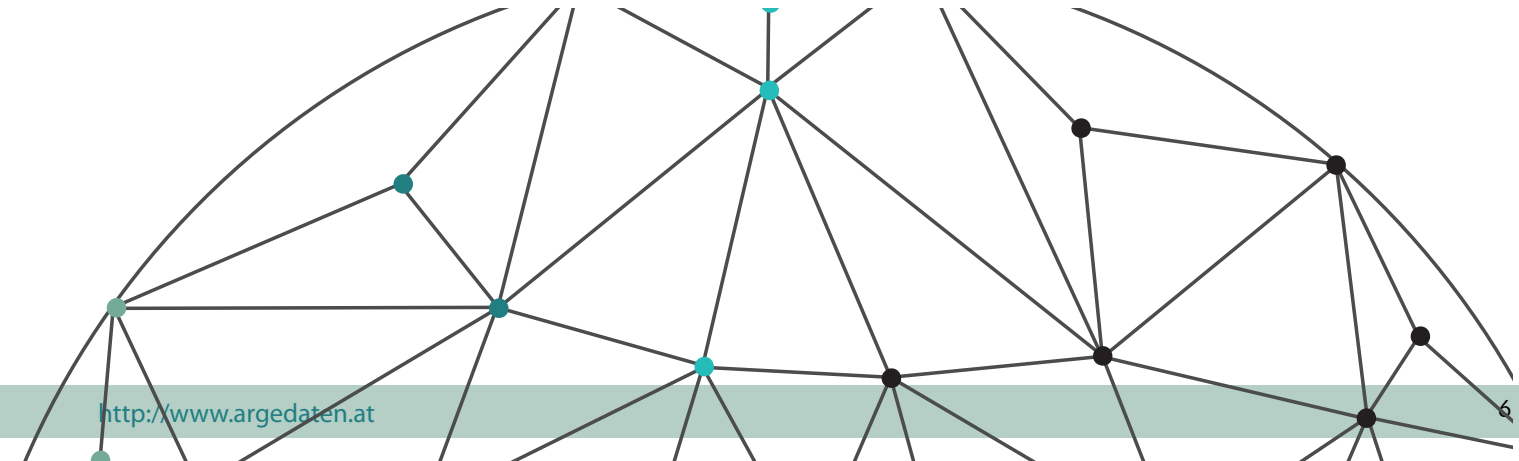
Die Datenschutzbehörde stellte zunächst fest, dass der Eingriff in das Grundrecht auf Geheimhaltung von Daten in mündlicher wie in schriftlicher Form erfolgen kann. Es wurde auch festgestellt, dass auch Schulnoten ein personenbezogenes Datum gem. Art. 4 Abs. 1 DSGVO.

NÄHERE INFORMATION ÜBER NOTE VERLETZT GEHEIMHALTUNGRECHT

Gegenstand des Gesprächs zwischen dem Lehrer und der Klassensprecherin war unter anderem auch eine detaillierte Information über das Zustandekommen der Note. Der Lehrer berief sich bei seiner Vorgehensweise auf § 6 Abs. 2 der Leistungsbeurteilungsverordnung, allerding ist das Vorgehen davon nicht gedeckt.

Der Lehrer brachte auch vor, keine neuen Informationen weitergegeben zu haben, dem konnte keine Folge geleistet werden. Die Datenschutzbehörde ging davon aus, dass der Klassensprecherin die genaue Notenzusammensetzung sicherlich nicht bekannt gewesen war und die Mitteilung sehr wohl neue Informationen enthielt. Die Schutzwürdigkeit der Daten war somit zu bejahen.

Es wurde nicht außer Acht gelassen, dass die Information über die Zusammensetzung der Note nur für die Bereinigung der Unstimmigkeiten an die Klassensprecherin mitgeteilt wurde. Jedoch stellt es kein gelindertes Mittel dar. Aus diesem Hintergrund gelangte die Datenschutzbehörde zum Ergebnis, dass eine Verletzung im Recht auf Geheimhaltung vorlag.



VERÖFFENTLICHUNG VON KONTAKTDATEN VERLETZT DAS RECHT AUF GEHEIMHALTUNG

Im Bescheid (DSB-D123.032/0003-DSB/2018) vom 19. August 2019, hatte sich die Datenschutzbehörde mit einer behaupteten Verletzung im Recht auf Geheimhaltung nach § 1 DSG zu befassen.

Ein Verband veröffentlichte personenbezogene Daten (Name, Telefonnummer, E-Mail-Adresse) eines Mannschaftstrainers auf der offiziellen Webseite. Das sollte, nach Aussagen des Verbandes, der Erleichterung der Kommunikation zwischen den Mannschaften dienen. Auf der Webseite existierte auch ein mit Login-Daten geschützter Bereich für Mitglieder. Der Beschwerdeführer rügte unberechtigte Verarbeitung von personenbezogenen Daten.

VERLETZUNG, WENN DATEN NICHT FÜR ÖFFENTLICHEN KONTAKT BESTIMMT SIND

Im Spruch gab die Datenschutzbehörde der Beschwerde statt und stellte die Verletzung des Rechts auf Geheimhaltung fest, da der Verband Namen, Telefonnummer und E-Mail-Adresse des Beschwerdeführers auf der Webseite im öffentlichen Bereich bekannt gab.

Die Veröffentlichung von Daten verletzt die Gemeinhaltungspflicht nach § 1 Abs. 1 DSG. Das vom Beschwerdeführer angeführte berechtigte Interesse gem Art. 6 Abs. 1 lit f DSGVO lag nicht vor.

Die Tatsache, dass die Kommunikation untereinander dadurch erschwert werde, dass sich berechtigte Personen vorab einloggen und die Kontaktdaten aus dem internen Bereich der Website beziehen müssten, überwiegt nach Ansicht der Datenschutzbehörde nicht das Grundrecht des Beschwerdeführers auf Geheimhaltung seiner personenbezogenen Daten.

WANN LIEGT EIN BERECHTIGTES INTERESSE VOR?

Das Prüfungsschema des Art. 6 Abs. 1 lit f DSGVO nach Kastelitz/Hötzendorfer/Tschohl im Knyrim, DatKomm Art. 6 DSGVO

1. Vorliegen eines berechtigten Interesses, was vom Verantwortlichen oder einem Dritten wahrgenommen wird.

2. Erforderlichkeit der Verarbeitung von personenbezogenen Daten zur Verwirklichung des berechtigten Interesses

3. Kein Überwiegen der Grundrechte und Grundfreiheiten der betroffenen Person.

Das Interesse an der Verarbeitung muss das Interesse an der Geheimhaltung überwiegen.

TIKTOK - WO BLEIBT DER KINDERSCHUTZ?

TikTok zählt zu den angesagtesten Apps 2019/20. Laut eigenen Angaben liegt die Nutzeranzahl aktuell bei 800 Mio. Das Prinzip funktioniert ganz einfach, es werden kurze Videos mit der zur Verfügung gestellten Musik aufgenommen, dazu wird oft gesungen und getanzt. Naheliegend ist es, dass die App bei minderjährigen Nutzern sehr beliebt ist. Das wirft datenschutzrechtliche Fragen auf.

Der Anbieter aus China verarbeitet laut Datenschutzerklärung Daten wie Kontaktdaten (Name, E-Mail, Telefonnummer), technische Daten (Gerätinformation, Gerätmodell, Zeitzone), IP-Adresse, hochgeladene Fotos und Videos, Inhalte versendeter Nachrichten, Kommentare und Likes. In die Verarbeitung von personenbezogenen Daten kann grundsätzlich gem Art. 6 Abs. 2 lit a DSGVO eingewilligt werden. Rechtmäßig ist die Einwilligung ab dem 16 Lebensjahr, davor bedarf es der Zustimmung des gesetzlichen Vertreters (Art. 8 Abs 1).

Die DSGVO erlaubt den Mitgliedstaaten abweichende Regelungen zu treffen, davon hat österreichischer Gesetzgeber Gebrauch gemacht. Nach DSG ist die Einwilligung bereits mit vollendetem vierzehnten Jahr rechtmäßig (§ 4 Abs. 4 DSG). Die Regelung lässt TikTok unbeeindruckt, das die Nutzungsfreigabe bereits ab 13 Jahre erlaubt. Jüngere Nutzer müssen die elterliche Einwilligung einholen, so der Anbieter. Nur wird da kaum ein Jugendlicher dabei sein, der die Eltern um Erlaubnis fragt. Oft wissen die Eltern nicht, welche Apps ihr Nachwuchs nutzt und welche Daten in den Tiefen des Internets verschwinden.

VERLORENE DATEN VERPFLICHTEN ZUR VERSTÄNDIGUNG DES BETROFFENEN

In der Entscheidung (DSB-D084.133/0002-DSB/2018) vom 8. August 2018 befasste sich die Datenschutzbehörde mit dem Schutz der Gesundheitsdaten.

Ein Rettungsdienst verlor das Suchtgiftbuch, welches nicht mehr aufgefunden werden konnte. Darin waren Daten von 150 Patienten enthalten (Vor-/ Nachname, körperliche Gesundheit, verabreichte, ausgegebe Suchmittelmenge), Datensätze von sieben externen Ärzten (Personalnummer, Unterschrift) sowie Datensätze von fünfzig Notfallsanitätern (Personalnummer, Unterschrift). Der Verantwortliche kam seiner Meldepflicht gegenüber der Aufsichtsbehörde gem Art. 33 DSGVO nach, unterließ aber die Benachrichtigung der Betroffenen und begründete dies damit, dass die weitere Verarbeitung oder Nutzung der Daten in „falschen Händen“ nur mit weiterer Recherche mögliche wäre. Deswegen liege kein potentiell hohes Risiko für Datenmissbrauch vor.

Dem Verantwortlichen wurde aufgetragen, innerhalb einer Frist von vier Wochen jene Personen zu benachrichtigen, deren Gesundheitsdaten von der Sicherheitsverletzung betroffen wurden.

GESUNDHEITSDATEN BESONDERS GEFÄHRDET

Im gegenständlichen Fall ist von der Sicherheitsverletzung eine umfangreiche Verarbeitung von Gesundheitsdaten umfasst. Die drohende Schadensschwere ist demnach hoch. Die Eintrittswahrscheinlichkeit für einen möglichen Schaden ist gegeben, da das Suchtgiftbuch nicht wiedergefunden wurde. Es entbehrt nicht jeder Lebensrealität, dass das Suchtgiftbuch von einem Unbefugten gefunden wurde bzw. noch gefunden wird. Die Gesundheit ist im Erwägungsgrund 75 DSGVO ausdrücklich hervorgehoben. Die Benachrichtigung ist nicht mit einem unverhältnismäßigen Aufwand gem Art. 34 Abs. 3 lit c DSGVO verbunden.

RISIKO DER DATENSCHUTZVERLETZUNG RICHTET SICH NACH GEFÄHRDUNG

Die Schwere des Risikos für die Rechte des Betroffenen beurteilt sich nach dem Gewicht des bedrohten Rechts. Als hoch wird die Schadensschwere dann eingestuft, wenn eine große Anzahl von Personen betroffen ist, große Mengen personenbezogener Daten, sensible Daten wie Gesundheit, wirtschaftliche Lage, persönliche Vorlieben und Interessen, Sexualleben, strafrechtliche Verurteilungen erfasst werden. (Erwägungsgrund 75 DSGVO)

In ihrer Entscheidung erwähnt DSB nur die gesundheitlichen Aspekte. Daraus lässt sich schließen, dass nur Patienten benachrichtigt werden sollen und nicht auch externe Mitarbeiter und Sanitäter, da von diesen im Suchtbuch nur die Personalnummer und die Unterschrift notiert waren.

KANN BENACHRICHTIGUNG UNTERBLEIBEN?

Die Benachrichtigung von betroffenen Personen kann nach Art. 34 Abs. 3 DSGVO dann unterbleiben, wenn der Verantwortlichen die geeigneten technischen und organisatorischen Sicherheitsvorkehrungen getroffen und angewendet hat, indem der Zugang zu personenbezogene Daten für Unbefugte unzugänglich gemacht wurde. Wenn das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen mit aller Wahrscheinlichkeit nicht besteht, oder individuelle Information mit einem unverhältnismäßigen Aufwand verbunden wäre. Dann hat die öffentliche Bekanntmachung oder ähnliche Maßnahme zu erfolgen.

UNVERLANGTE E-MAIL ZUSENDUNG ZU WERBEZWECKEN IST DATENSCHUTZVERLETZUNG

In der Entscheidung (DSB-D130.033/0003-DSB/2019) vom 7.3.2019 beschäftigte sich die Datenschutzbehörde mit Zulässigkeit von Werbemails.

Im Jahr 2014 meldete sich der Beschwerdeführer für eine Marketingveranstaltung des Beschwerdegegners an. Im Mai 2018 erhielt er eine E-Mail mit der Bitte eine Einwilligung zu erteilen, falls weiterer Kontakt erwünscht ist. Die Einwilligung wurde nicht erteilt. Im Juni 2018 erhielt der Beschwerdeführer ein personalisiertes Werbemail (Angebot zur Teilnahme an einer Eventveranstaltung in DE).

Die Datenschutzbehörde gab der Beschwerde statt und stellte eine Verletzung im Grundrecht auf Geheimhaltung fest.

MÖGLICHKEITEN DER DATENSCHUTZBESCHWERDE

Im vorliegenden Fall wurde die E-Mail zu Werbezwecken verschickt. Bei Zusendung von elektronischer Post zu Werbezwecken ohne Einwilligung kommt § 107 Abs. 1 TKG 2003 zur Anwendung. Dem Beschwerdeführer steht trotzdem eine Datenschutzbeschwerde nach Art. 77 Abs. 1 DSGVO offen, weil gleichzeitig eine Verletzung des Rechts auf Geheimhaltung nach § 1 Abs. 1 DSG vorliegt.

ZUSTIMMUNG NICHT IMMER ERFORDERLICH

Keiner vorherigen Zustimmung bedarf es, wenn die Kontaktinformationen im Zusammenhang mit Verkauf oder Dienstleistung von Kunden erhalten wurden, die Nachricht der Direktwerbung für eigene ähnliche Produkte dient, der Empfänger klar und deutlich die Möglichkeit bekommen hat, diese kostenfrei abzulehnen und der Empfänger die Zusendung nicht von vornherein angelehnt hat. Die Voraussetzungen müssen kumulativ vorliegen.

Die Ausnahmen des § 107 Abs. 3 TKG 2003 kommen nicht zur Anwendung, weil der Kunde keine Möglichkeit erhalten hat, die Nutzung elektronischer Kontaktinformation von vornherein abzulehnen.

MANGELHAFTE ANONYMISIERUNG VON DATEN FÜHRT ZUR AUSKUNFTSPFLICHT

In der Entscheidung (DSB-D123.224/0004-DSB/2018) beschäftigte sich die Datenschutzbehörde mit der Frage der unzureichenden Anonymisierung von Daten.

Die Beschwerdegegnerin erstellte eine Stellungnahme zum Thema „Fragen zu Doppelansässigkeit in Österreich und Schweiz". Dafür verwendete sie solche Daten wie Wohnort, familiäre und wirtschaftliche Situation, soziale Kontakte, Interessen, Hobbys, die Zugehörigkeit zu Clubs und Stammrunden. Für die Erhebung dieser Daten wurden keine eigenen Sachverhaltserhebungen durchgeführt, sondern vom jeweiligen Auftraggeber übermittelt. Beschwerdeführerin stellt einen Antrag auf Erteilung der Auskunft. Beschwerdegegnerin behauptet keine personenbezogenen Daten verarbeitet zu haben, da es sich bei verarbeiteten Daten um anonymisierte Informationen handelte.

Die Datenschutzbehörde gab der Beschwerde statt und stellte die Verletzung des Rechts auf Auskunft fest.

PSEUDOANONYMISIERUNG VS. ANONYMISIERUNG

Aufgrund der Kombination von mehreren Eigenschaften kann der Kreis der potenziellen Betroffenen soweit eingeschränkt werden, dass die Beschwerdeführerin eindeutig identifiziert werden kann. Für die Identifikation bedarf es auch keinen großen Aufwandes.

Die verwendeten Daten sind nicht anonym, sondern pseudoanonym da die immer noch auf eine bestimmte Person zurück geführt werden können. Die Pseudonymisierung hat keine Wirkung auf den Personenbezug der Daten, da dem Verantwortlichen weiterhin der vollständige Informationsgehalt der Daten zur Verfügung steht und der individuelle Bezug ohne großen Aufwand hergestellt werden kann.

Nach Legaldefinition ist „Pseudonymisierung" dann gegeben, wenn die personenbezogenen Daten ohne Zuziehen weiterer zusätzlicher Informationen nicht mehr auf eine bestimmte Person zurückzuführen sind. Die zusätzlichen Informationen müssen dafür gesondert aufbewahrt werden.

Im Gegensatz dazu kann bei anonymisierten Daten die Personenbezogenheit der Daten nicht mehr, oder nur mit erheblichem, der Allgemeinheit nicht möglichem Aufwand hergestellt werden. Auf die anonymisierten Informationen findet DSGVO oder sonstige datenschutzrechtliche Materien keine Anwendung (ErwG 26).

GEHEIMHALTUNG BEI GRUNDBUCHSDATEN

Im Bescheid (D123.626/0006-DSB/2019) vom 23. April 2019 beschäftigte sich die Datenschutzbehörde mit der Frage, ob es zulässig ist personenbezogene Daten aus dem Grundbuch zu verwenden, um in weitere Folge die Eigentümer der Liegenschaften mit Kaufangeboten zu kontaktieren.

Die im Grundbuch erfassten sind personenbezogene Daten, die öffentlich zugänglich sind. Dabei handelt es sich offenkundig weder um sensible noch strafrechtlich relevante Daten. Aus diesem Grund ist von einer geringeren Schutzwürdigkeit auszugehen.

BERECHTIGTES INTERESSE BEI VERWENDUNG VON GRUNDBUCHSDATEN

Angeführt wurde auch das berechtigte Interesse des Immobilientreuhänders laufend Liegenschaften bzw. Grundstücke zu erwerben und damit verbundenes wirtschaftliches Interesse.

Die Datenschutzbehörde nahm die Interessenabwägung vor und kam zum Ergebnis, dass kein Recht auf Geheimhaltung vorliegt, da das berechtigte Interesse der Beschwerdeführerin als Immobilientreuhänder überwiegt. Zudem wurde die Beschwerdeführerin lediglich nur einmal von dem Immobilientreuhänder kontaktiert. Ferner hat die Beschwerdegegnerin auch angeboten, die personenbezogenen Daten zu löschen bzw. weitere Kontaktaufnahme zu unterlassen.

BEI WIEDERHOLTEM KONTAKT KEIN BERECHTIGTES INTERESSE

Anders entschied die Datenschutzbehörde im Bescheid von 20. Mai 2019 (GZ: DSB-D123.972/0005-DSB/2019) beim mehrmaligen Kontakt durch den Immobilientreuhänder.

Konkret wurde der Beschwerdeführer im Zeitraum von einem Jahr drei Mal kontaktiert, um dessen Verkaufsabsichten zu ermitteln. Hier fiel die Interessenabwägung zugunsten des Beschwerdeführers aus, welcher ein berechtigtes Interesse daran hat, dass seine personenbezogenen Daten nicht dauerhaft zum Zweck regelmäßiger Anfragen verarbeitet werden. Die Verletzung des Rechts auf Geheimhaltung lag demnach vor.

LÖSCHUNG VON GESPEICHERTEN DATEN WÄHREND DES AUSKUNFTSVERFAHRENS

In der Entscheidung (DSB-D124.071/0005-DSB/2019) vom 27. Juni 2019 beschäftigte sich die Datenschutzbehörde mit der Zulässigkeit der Datenlöschung während des laufenden Auskunftsverfahrens.

Zum Zeitpunkt der Antragstellung auf Auskunftsbegehren verarbeitet die Beschwerdegegnerin die personenbezogenen Daten des Beschwerdeführers. Nach Kenntnis des Auskunftsbegehrens vernichtete diese sämtliche den Beschwerdeführer betreffende personenbezogenen Daten. Noch am selben Tag teilte die Beschwerdegegnerin mit, dass keine personenbezogenen Daten verarbeitet werden.

Die Datenschutzbehörde gab der Beschwerde statt und stellte fest, dass die Beschwerdegegnerin den Beschwerdeführer dadurch im Recht auf Auskunft verletzt hat, indem sie nach Eingang des Auskunftsbegehrens dessen personenbezogene Daten gelöscht bzw. vernichtet und danach Negativauskunft erteilt hat.

KEIN AUSDRÜCKLICHES LÖSCHUNGSVERBOT NACH DSGVO

DSGVO enthält im Gegensatz zu § 26 Abs. 7 DSG 2000 kein ausdrückliches Löschverbot. Die Vorgehensweise des Beschwerdegegners nach Eingang des Auskunftsbegehrens entspricht trotzdem nicht dem Grundsatz der Verarbeitung nach Treu und Glauben und stellt damit eine Verletzung des Rechts auf Auskunft des Beschwerdeführers dar (Art. 15 iVm Art. 5 Abs. 1 lit. a DSGVO).

LÖSCHUNG VERLETZT GRUNDSATZ VON TREU UND GLAUBEN

Nach Art. 5 Abs. 1 lit a DSGVO müssen personenbezogenen Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffenen Personen nachvollziehbaren Weise, verarbeitet werden (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz).

Der Grundsatz Treu und Glauben stellt gewissermaßen eine Auffangklausel dar, welche insbesondere bei der Durchführung von Interessenabwägungen zu berücksichtigen ist (Forgó / EU DSGVO Kommentar).

Auch die Transparenz kann nach der Löschung der Daten nicht mehr überprüft werden. Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist (Erwägungsgrund 58).

BEWEGUNGSMELDER IN REHABILITATIONSKLINIK

In der Entscheidung (DSB-D123.942/0004-DSB/2019) der Datenschutzbehörde wurde die Zulässigkeit von Bewegungsmeldern überprüft. Diese wurden zum Zweck der elektronischen Zimmerbelegungserkennung in einem Rehabilitationszentrum installiert.

Der Beschwerdeführer befürchtete, dass mit Hilfe von Daten Bewegungsprofile erstellt werden, was zum Zweck der Heilbehandlung nicht notwendig ist. Die Beschwerdegegnerin brachte vor, dass aus diesen Daten keine Bewegungsprofile erstellt werden können. Die Daten liefern ausschließlich nur Information, ob sich ein Patient im Zimmer befindet oder nicht.

Die Datenschutzbehörde hat die Beschwerde abgewiesen und es mit der Mitwirkungspflicht des Patienten begründet. Das Ziel des Aufenthalts in Sonderkrankenanstalten ist die Verbesserung der individuellen gesundheitlichen Probleme. Dazu zählt auch die Einhaltung der vorgeschriebenen Nachtruhe. Die Bewegungsmelder dienen nur der Feststellung der Anwesenheit im Zimmer nach 22:30. Die Verarbeitung von Daten ist auf Grund des berechtigten Interesses zulässig, da es sich dabei um keine personenbezogenen gesundheitlichen Daten handelt.

ARTEN VON PERSONENBEZOGENEN DATEN

Die DSGVO unterscheidet die Verarbeitung von personenbezogenen Daten der einfachen (Art. 6 DSGVO) und besonderen Kategorie (Art. 9 DSGVO).

Die Verarbeitung von „einfachen" personenbezogenen Daten ist dann rechtmäßig, wenn die Bedingungen des Art. 6 Abs 1 ff DSGVO erfüllt sind. Lit f erlaubt die Verarbeitung von Daten beim Vorliegen berechtigten Interesses des Verantwortlichen, sofern die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.

Nach Art. 9 Abs. 1 DSGVO sind personenbezogenen Daten besonderer Kategorie solche, die über rassische und ethnische Herkunft, religiöse oder weltanschauliche Überzeugung, biometrische und gesundheitliche Daten Auskunft geben. Die Verarbeitung solcher Daten wird - mit Ausnahmen - untersagt.

Abs. 1 gilt dann nicht, wenn zum Beispiel eine ausdrückliche Einwilligung des Betroffenen vorliegt, die Verarbeitung aus Gründen des Arbeitsrechts und der sozialen Sicherheit erforderlich ist, die dem Schutz von lebenswichtigen Interessen dient oder die Person personenbezogenen Daten offensichtlich öffentlich gemacht hat. Das berechtigte Interesse kann bei personenbezogenen Daten der besonderen Kategorien nicht geltend gemacht werden.

Auch in Fällen von Epidemie wie im Corona-Fall können Gesundheitsdaten an die Behörde weitergegeben werden, es bedarf aber gesetzlicher Genehmigung.

GESUNDHEITSDATEN UNTERLIEGEN BESONDEREM SCHUTZ

Im vorliegenden Fall führt die DSB aus, dass die von dem Rehabilitationszentrum verarbeitete Daten nicht als gesundheitsbezogenen Daten zu werten sind.

Welche Daten als gesundheitsbezogen zu qualifizieren sind, ist aus dem ErwG 35 DSGVO ersichtlich. Dazu zählen alle Daten, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen.

Dazu gehören auch Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese für gesundheitliche Zwecke eindeutig zu identifizieren.

Der Begriff „Gesundheit" ist weit auszulegen und betrifft nicht nur medizinische Diagnosen, sondern bezieht sich auf alle Informationen und Meinungsäußerungen, die die Gesundheit einer Person unter allen Aspekten körperlich wie psychisch betreffen. so der EuGH (vgl Urteil der EuGH vom 6. November 2003, C-101/01, Rs Lindqvist, Rz 50).

MEINUNGSSTREIT UM SOZIALVERSICHERUNGSNUMMER

In diesem Zusammenhang ist auch auf die Sozialversicherungsnummer einzugehen. Im früheren Erkenntnis entschied das Bundesverwaltungsgericht, dass die Sozialversicherungsnummer ohne Zweifel ein personenbezogenes Datum iSd Art 4 Z1 DSGVO darstellt (BVwG vom 11 Juni 2018, W211 2161456-1). Die Frage, ob die Sozialversicherungsnummer auch ein gesundheitsbezogenes Datum ist, löste großen Meinungsstreit aus, der bis heute nicht bereinigt wurde.

Nach überwiegender Meinung zählt die Sozialversicherungsnummer nicht zu gesundheitsbezogenen Daten. Die Sozialversicherungsnummer stellt zwar eine Nummer / ein Kennzeichen iSd ErwG 35 DSGVO dar, die einer natürlichen Person zugeteilt wurde. Allerdings müssen sich nach Art. 4 Abs. 1 Z 15 die Gesundheitsdaten auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen, aus denen Informationen über deren Gesundheitszustand hervorgehen. Da aus SV-Nummer kein direkter Bezug auf Informationen über den Gesundheitszustand genommen werden kann, sind diese nicht als gesundheitsbezogene Daten zu qualifizieren.

Es kann auch davon abhängig gemacht werden, im welchen Zusammenhang die Sozialversicherungsnummer verwendet wird. Wenn diese im Zusammenhang mit Gesundheitsdienstleistungen verwendet wird, kann die Verarbeitung in die Kategorie besonders geschützter Daten fallen. Allerdings nicht bei Inanspruchnahme von Sozialleistungen, wie etwa in Angelegenheiten der Arbeitslosenversicherung, in diesem Fall wird die Sozialversicherungsnummer zur bloßen Identifikationsnummer (vgl Hödl in Knyrim (Hrsg), DatKomm Art. 4 Rz 157).

Es wird auch die alternative Meinung vertreten, dass die Sozialversicherungsnummer gänzlich in die Kategorie besonders geschützter Daten fällt, wenn man wenigstens davon ausgeht, dass die der eindeutigen Identifizierung der betroffenen Person diene (vgl Feiler/Forgó, EU-DSGVO Art. 4 Rz 36).

EUGH: LÖSCHUNG PERSONENBEZOGENER DATEN IN ALLEN EU-VERSIONEN VON GOOGLE

Der Ausgangspunkt des Verfahrens (C-507/17) war der Rechtsstreit zwischen Google und der französischen Datenschutzbehörde CNIL darüber, wie Suchmaschinen das Recht auf Auslistung umsetzten sollen. Das Recht auf Auslistung oder „Recht auf Vergessenwerden" wurde vom Gerichtshof im Urteil vom 13. Mai 2014, Google Spain und Google (C-131/12) anerkannt.

Nach der Einreichung des Vorabentscheidungsverfahrens erklärte Google vor dem europäischen Gerichtshof, dass sie die neue Darstellung der nationalen Version ihrer Suchmaschine eingeführt haben. Die Internetnutzer werden nun automatisch auf die nationale Version der Suchmanische von Google geleitet. Die Suchergebnisse werden nach Maßgabe des Ortes angezeigt, der von Google mittels Geolokalisierung ermittelt wurde.

RECHTS AUF LÖSCHUNG GEGEN NIEDERGELASSENEN SUCHMASCHINENBETREIBER

Vor diesem Hintergrund musste unter anderem die Frage geklärt werden, ob der Suchmaschinenbetreiber beim Löschungssantrag die Auslistung in allen Versionen oder nur in der Version des jeweiligen Staates seiner Suchmaschine vornehmen muss.

Im Rahmen der DSGVO ergibt sich das Auslistungsrecht der betreffenden Personen nun aus Art. 17 der Verordnung.

Aus Art. 4 Abs. 1 lit. a der Richtlinie 95/46 sowie aus Art. 3 Abs. 1 der Verordnung 2016/679 folgt, dass die betroffene Person ihr Recht auf Auslistung gegenüber demjenigen Suchmaschinenbetreiber geltend machen kann, der eine oder mehrere Niederlassungen im Gebiet der Union besitzt, unabhängig davon, ob die Verarbeitung in der Union stattfindet oder nicht. Somit sind Tätigkeiten des Suchmaschinenbetreibers und die seiner Niederlassung untrennbar miteinander verbunden.

Im vorliegenden Fall hat Google seine Niederlassung im französischen Hoheitsgebiet und übt insbesondere gewerbliche und Werbetätigkeiten aus.

LÖSCHUNG IN JEDER EU-VERSION

Räumlich gesehen beschränkt sich das Auslistungsrecht nur auf das Hoheitsgebiet der Union. Der Grund dafür ist, dass viele Drittstaaten ein Auslistungsrecht gar nicht kennen, zudem ist das Recht auf Schutz personenbezogener Daten kein uneingeschränktes Recht, sondern muss unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden.

Aus Art. 17 Abs. 1 DSGVO konnte bisher keine Verpflichtung für den Suchmaschinenbetreiber abgeleitet werden,der die Auslistung in allen Versionen seiner Suchmaschine vornehmen muss.

Damit räumte der EuGH auf und stellte in seiner Entscheidung klar, dass die Auslistung in allen mitgliedstaatlichen Versionen der Suchmaschine vorgenommen werden muss. Er begründete dies damit, dass der Unionsgesetzgeber sich dafür entschieden hat, den Datenschutz in einer einzigen Verordnung zu regeln, die in jedem Mitgliedstaat unmittelbar anwendbar ist. Das Ziel laut dem Erwägungsgrund 10 der Verordnung ist die gleichwertige Gewährleitung des hohen Datenschutzniveaus für alle Mitgliedstaaten der Union.

ZEITAUFZEICHNUNG MITTELS FINGERABDRUCK OHNE EINWILLIGUNG UNZULÄSSIG

Das Arbeitsgericht Berlin entschied über die Zulässigkeit der Zeitaufzeichnung mittels Fingerabdruck (29 CA 5451/19).

In einem Rundmail wurde allen Mitarbeiter mitgeteilt, dass die Arbeitszeiten in der Zukunft ausschließlich nur mit dem neuen Zeitaufzeichnungssystem, das die Arbeitszeiten mittels Fingerabdruck dokumentiert, vorgenommen werden. Frühere händische Aufzeichnungen werden nicht mehr anerkannt.

Der Kläger erteilte weder die Einwilligung noch nutzte er das neue Zeitaufzeichnungssystem und wurde in der Folge durch den Arbeitgeber drei Mal abgemahnt. Der Kläger begehrte in seiner Klage die Entfernung der drei Abmahnungen aus der Personalakte.

Durch das neue System meldeten sich die Mitarbeiter mit einem Fingerabdruck an und ab. Dafür wurden von dem Fingerabdruck zunächst sogenannte Minutien (individuelle, nicht vererbbare Fingerlinienverzweigungen) mittels speziellen Algorithmus erfasst. Aus dem gespeicherten Minutiendatensatz kann der Fingerabdruck des Mitarbeiters nicht wieder generiert werden.

VERARBEITUNG VON BIOMETRISCHEN DATEN

Bei Minutiendatensatz handelt es sich um biometrische Daten nach Art. 9 Ans 1 DSGVO. Die Verarbeitung solcher Daten ist nach Art. 9 Abs. 1 grundsätzlich verboten. Art. 9 Abs. 2 DSGVO enthält Fälle, die Verarbeitung in Ausnahmefällen zulassen. Arbeitsrechtlich relevante Erlaubnistatbestände sind solche wie „Erforderlichkeit", „freiwillige Einwilligung" und „Kollektivvereinbarung". In dem dargestellten Fall lag keine kollektivvertragliche Vereinbarung vor.

ERFORDERLICHKEIT NUR BEI WICHTIGEM INTERESSE DES ARBEITGEBERS

Die Erforderlichkeit bei Verarbeitung liegt laut Gericht dann vor, „wenn es zu Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses notwendig ist".

Je intensiver der Eingriff in das Persönlichkeitsrecht ist, desto schwerer muss der vom Arbeitgeber verfolgte Zweck wiegen. Bei Zugangskontrolle mittels biometrischer Daten zu Bereichen mit sensiblen Geschäfts-, Produktions- und Entwicklungsgeheimnisse kann das Interesse des Arbeitgebers überwiegen, bei bloßen Zeitaufzeichnungen im Büro jedoch nicht.

Auch das mögliche „mitstempeln" durch Arbeitskollegen begründet die Erforderlichkeit nicht, da in der Regel davon auszugehen ist, dass die überwiegende Anzahl der Arbeitnehmer sich rechtstreu verhält.

In Österreich wurde eine ähnliche Entscheidung (9 ObA 109/06d) vom OGH, unter Mitwirklung von ARGE DATEN, bereits am 20.12.2006 gefällt.

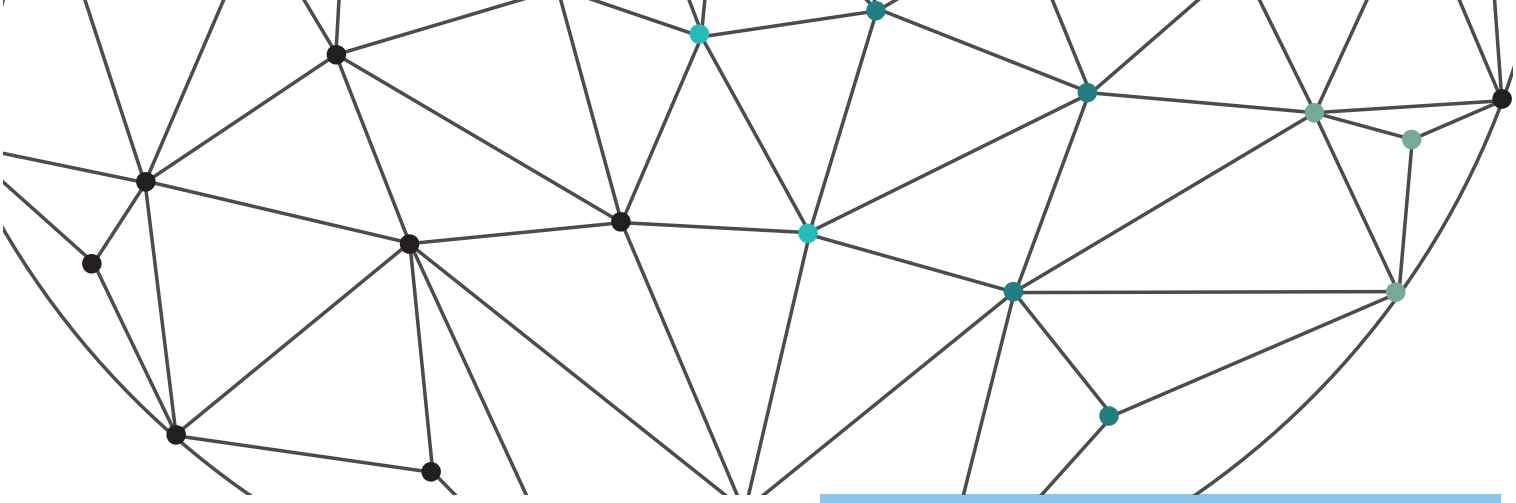
ALEXA - DER (UN)GEBETENE GAST

„Computer, wie wird das Wetter heute?". Die Sprachassistenten wie Google Home, Alexa, Siri gehören mittlerweile in vielen Familien zum Mobiliar. Dabei ist es lange kein Geheimnis mehr, dass die Sprachkommandos aufgezeichnet und in weiterer Folge von jeweiligen Anbietern ausgewertet werde. Begründet wird dies mit Verbesserung und Anpassung der Geräte an die Nutzer.

Grundsätzlich aktiviert sich der Sprachassistent mit dem persönlich ausgewählten Aktivierungswort und zeichnet nur dann die Kommandos auf. Es kam aber schon vermehrt zu Fällen der unaufgeforderten Sprachaufzeichnung. Die Anbieter leugnen diese Tatsache auch nicht, dafür reicht schon ein Blick in die Datenschutzbestimmungen, die genau dieses Thema ansprechen. Von dieser Schwachstelle wissen auch die Strafverfolgungsbehörden. In den USA wurden bereits drei Mal die Audioaufnahmen von Amazons Sprachassistenten „Alexa" für die Aufklärung von Verbrechen an die Polizei übergeben.

Auch in Deutschland wird über die Möglichkeit der Auswertung von Audioaufnahmen in Strafprozessen diskutiert. Ob solche Diskussionen auch in Österreich aktuell werden, lässt sich nicht beantworten. Sollte sich jedoch der Zugriff von Behörden auf Audioaufnahmen solcher Art ermöglicht werden, hätte man ganz schnell einen ungebetenen Gast bei sich auf dem Küchentisch.

Wie viel Privatsphäre sind wir also bereit für die Bequemlichkeit aufzugeben?



UNZULÄSSIGE ERHEBUNG VON DATEN BEI KONFERENZEN

In der Entscheidung (DSB-D123.311/0003-DSB/2019) der Datenschutzbehörde vom 21. Februar 2019 ging es um die Daten, die in einem Akkreditierungsverfahren erhoben wurden.

Der Beschwerdeführer meldete sich für eine Konferenz des Bundesministeriums für Nachhaltigkeit und Tourismus an. Bei der Anmeldung gab er Vor- und Nachnamen, Geburtsdatum, Geschlecht, Nationalität, Delegations- bzw. Organisationsnamen, E-Mail-Adresse, Foto für den Badge sowie ein gültiges Ausweisdokument bekannt.

In späterer Folge stellte sich heraus, dass es sich dabei um keine Veranstaltung mit Sicherheitsprüfung handelte. Für Veranstaltungen ohne Sicherheitsprüfung ist die Angabe von Vor- und Nachnamen, E-Mail-Adresse, Foto sowie Scan eines gültigen Ausweisdokuments ausreichend. Der Beschwerdeführer bringt daher vor, dass keine freiwillige Einwilligung in die Datenverarbeitung vorlag.

KEINE FREIWILLIGKEIT BEI EINWILLIGUNG

Dem Beschwerdeführer wurde keine Wahlfreiheit gelassen, nur jene Daten bereit zu stellen, die für die Teilnahme an dieser Veranstaltung unbedingt erforderlich sind, sondern es wurden alle Daten ermittelt, die auch Personen bereitstellen müssen, welche sich einer Sicherheitsüberprüfung unterziehen. Zudem bestand ein klares Ungleichgewicht, da es sich hier um einen Hilfsapparat der Behörde handelt. Die Freiwilligkeit lag daher nicht vor. Die Datenschutzbehörde stellte die Verletzung des Rechts auf Geheimhaltung fest.

BESCHRÄNKUNG AUF NOTWENIGES MASS AN DATEN

Der Verantwortliche hat sich auf das notwenige Maß bei der Datenanforderung zu beschränken. Im vorliegenden Fall wurden die Daten (Geschlecht, Nationalität, Delegations- bzw. Organisationsnamen) über den geforderten Zweck hinaus erfasst. Dadurch liegt ein Eingriff in Art 5 Abs 1 lit c DSGVO vor.

E-SCOOTER ERFASST BEWEGUNGSROUTEN

Mit dem Einzug der E-Scooter in die Großstädte wurde in den Medien über alle möglichen damit verbundene Probleme diskutiert. Der Datenschutz wurde mehr oder weniger außen vorgelassen.

Vielen Nutzern von E-Scooter-Diensten ist nicht bewusst, wie groß das Ausmaß an Daten ist, die der Anbieter erhebt. In den meisten Fällen werden die langen Datenschutzerklärungen beim Vertragsabschluss nicht gelesen. Dabei ist dazu dringend zu raten.

Erhoben werden Kontaktinformationen (Name, E-Mail-Adresse, Telefonnummer, Zahlungsdaten), Standortdaten, wenn der Nutzer sich anmeldet und die Dienste nutzt. Der Anbieter behält sich auch vor die Geräte während der Nutzung zu orten. So können ganz leicht die Bewegungsprofile zusammengestellt werden. Da die E-Scooter an Zielorten abgestellt werden, können persönliche Vorlieben und Tagesabläufe erstellt werden, die bei Analysen über Kunden- und Nutzungsverhalten interessant sind.

Solche Daten sind auch für Verkehrs- und Strafverfolgungsbehörden vom Interesse, weil sie für Verkehrsplanung oder sogar Aufklärung und Verfolgung von Ordnungswidrigkeiten genutzt werden können. Die Anbieter sind auch bereit die Daten auszufolgen, wenn „das aus rechtlichen Gründen vernünftigerweise notwendig ist".

Laut Datenschutzbestimmungen werden die Daten auch an Dienstleister, Partner und Dritte für Forschungs-, Geschäfts- oder andere Zwecke weitergegeben.

Auch die Dauer der Datenspeicherung ist schwammig umschrieben und gibt keine klare Aussage. Die Daten werden solange gespeichert, wie es für die Bereitstellung der Dienste notwendig ist oder bis zur Löschung des Nutzerkontos. Allerdings behält der Anbieter sich das Recht vor, auch nach Löschung die Informationen weiter zu speichern. Das heißt wohl, dass die Daten freiwillig nie gelöscht werden.

Fazit ist, wenn man auf die Nutzung von Mietscootern nicht verzichten kann oder möchte, sollten vor Eröffnung des Nutzerkontos die Datenschutzbestimmungen genau studiert werden. Da die Verarbeitung und Weitergabe von Daten sich von Anbieter zu Anbieter stark unterscheidet. Möglich ist natürlich auch, dass die Datenschutzbestimmungen bei den jeweiligen Anbietern nicht transparent genug sind.

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

DATENSCHUTZSTENOGRAMM 2019

17. DEZEMBER 2019
Belgische Aufsichtsbehörde (DOS-2019-04234): Die belgische Aufsichtsbehörde verhängte eine Strafe iHv 2000,- für nicht innerhalb der angesetzten Frist (20 Tage) erteiltes Auskunftsbegehren. Die Strafe soll der Abschreckung vor solchen Versäumnissen dienen.
https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/DEQF_13-2019_FR_ANO.pdf

11. DEZEMBER 2019
VfGH-Entscheidung (G72/2019): Die Datenspeicherung „auf Vorrat" ist nur zur Bekämpfung schwerer Kriminalität zulässig. Die angefochtene Bestimmung (§ 54 Abs. 4b SPG) erlaubte auch die Verarbeitung von Daten zur Verfolgung von leichter Vermögenskriminalität. Das stellt einen gravierenden Eingriff in die Geheimhaltungsinteressen (§ 1 DSG) und das Recht auf Privatleben (Art. 8 ERMK).
https://www.ris.bka.gv.at/Dokumente/Vfgh/JFR_20191211_19G00072_01/JFR_20191211_19G00072_01.html

11. DEZEMBER 2019
VfGH-Entscheidung: „Bundestrojaner" stellt einen schwerwiegenden Eingriff in das Grundrecht auf Privatsphäre dar. „Die vertrauliche Nutzung von Computersystemen und Nachrichtendiensten ist ein wesentlicher Bestandteil des Rechts auf Achtung des Privatlebens nach Art. 8 EMRK".
https://www.vfgh.gv.at/medien/Kfz-Kennzeichenerfassung_und__Bundestrojaner__verfass.de.php

9. DEZEMBER 2019
Bundesbeauftragter für Datenschutz (DE): Bußgeld in Höhe von 9,55 Mio für Telekommunikationsdienst 1&1 (nicht rechtskräftig). Dem Unternehmen wird vorgeworfen, an der Kundenhotline umfangreichende Informationen zu weiteren personenbezogenen Kundendaten herausgegeben zu haben.
https://newsroom.1und1.de/2019/12/09/11-klagt-gegen-bussgeldbescheid-der-datenschutzbehoerde/

27. NOVEMBER 2019
OGH-Entscheidung (6 Ob 217/19h): Die Beweislastumkehr bei Schadenersatzansprüchen nach Art. 82 DSGVO besteht nur hinsichtlich des Verschuldens. Beim Kausalitätszusammenhang und Schadensnachweis liegt die Nachweispflicht beim Betroffenen.
https://www.adresshandel-und-recht.de/urteile/Beweislast-bei-DSGVO-Schadensersatzanspruch-Oberster_Gerichtshof-20191127/

20. NOVEMBER 2019
BVwG-Entscheidung (W256 2214855-1): Ohne Kenntnis der konkreten Datenverarbeitung durch den Beschwerdegegner, kann die Verletzung des Rechts auf Datenschutz nicht festgestellt werden. Bloße Mutmaßung der mitbeteiligten Partei, sie werden von dem Beschwerdegegner anhand von Kameras überwacht, ist für die Behauptung der Rechtsverletzung nicht geeignet.
https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20191120_W256_2214855_1_00/BVWGT_20191120_W256_2214855_1_00.html

5. NOVEMBER 2019
Berliner Datenschutzbeauftragter: Strafe von 14,5 Mio für Deutsches Wohnen SE (nicht rechtskräftig). Nicht Löschen von Daten, die ihren Zweck nicht mehr erfüllen, stellt eine Datenschutzverletzung dar.
https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf

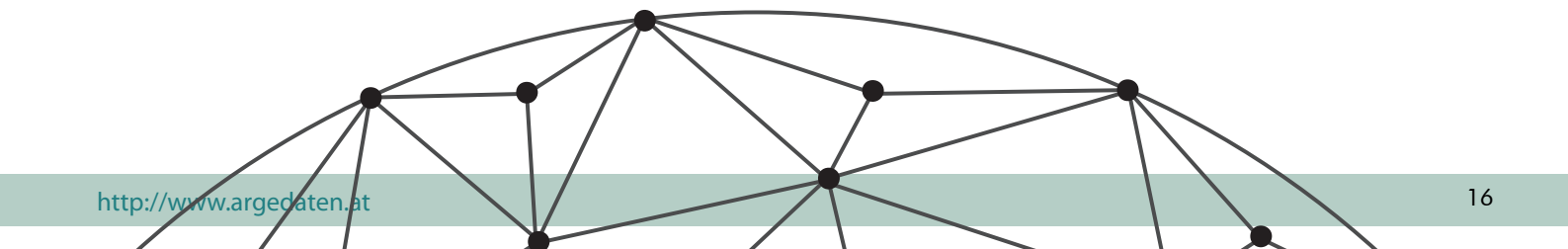
30. OKTOBER 2019
BVwG-Entscheidung (W258 2216873-1): Das Widerspruchsrecht, welches sich aus besonderer Situation des Betroffenen ergibt (Art. 21 Abs. 6 DSGVO), kann unwirksam sein. Werden die besonderen Gründe nicht genauer erläutert oder nur darauf verwiesen, dass die Daten „alt" oder „unrichtig" sind, ist der Widerspruch unwirksam.
https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20191030_W258_2216873_1_00/BVWGT_20191030_W258_2216873_1_00.html

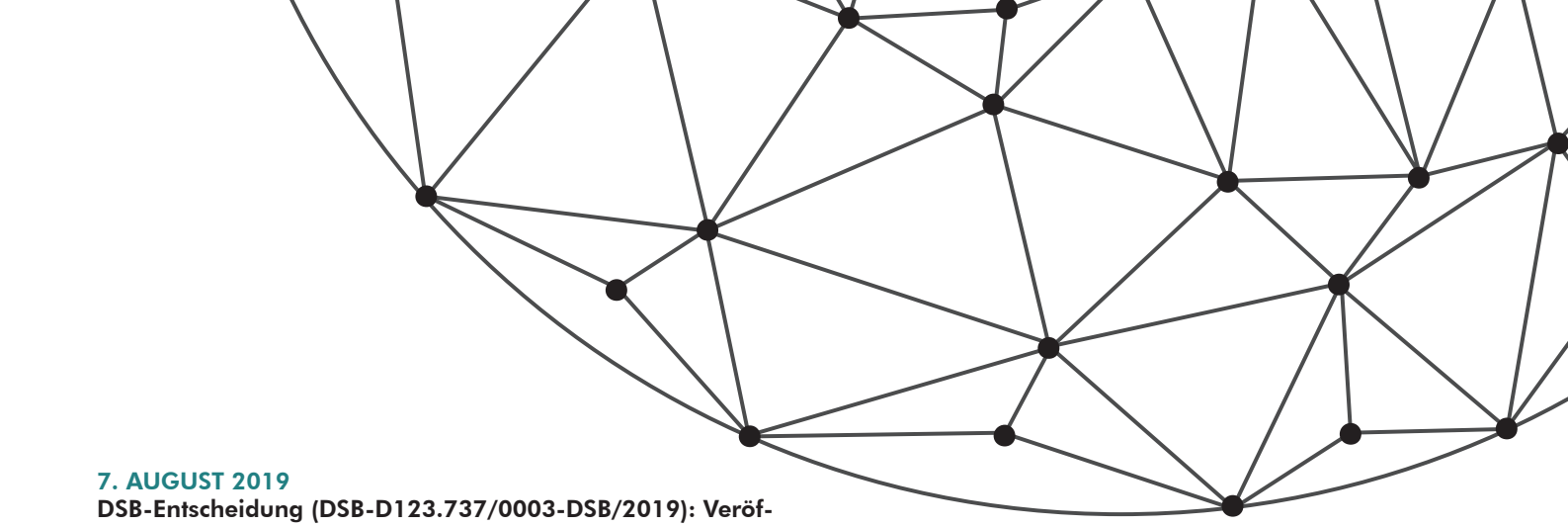
30. OKTOBER 2019
BVwG-Entscheidung (W258 2218465-1): Als Richtlinie über die zulässige Speicherdauer von Bonitätsdaten eines Schuldners können Beobachtungs- und Löschungsfristen in rechtlichen Bestimmungen herangezogen werden, die dem Gläubigerschutz dienen oder die Erfordernisse an eine geeignete Bonitätsbeurteilung näher festlegen.
https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20191030_W258_2218465_1_00/BVWGT_20191030_W258_2218465_1_00.html

10. OKTOBER 2019
DSB-Entscheidung (DSB-D124.1078/0001-DSB/2019): Eine sukzessive Inanspruchnahme der Datenschutzbehörde in derselben Sache kommt nicht in Betracht, wenn darüber bereits ein rechtskräftiger und vollstreckbarer Rechtsbehelf eines Gerichts vorliegt. Da es nicht der Zweck der DSGVO sein kann eine parallele oder sukzessive Verfahrensführung vor einer Aufsichtsbehörde und einem Gericht zu ermöglichen.
https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20191010_DSB_D124_1078_0002_DSB_2019_00/DSBT_20191010_DSB_D124_1078_0002_DSB_2019_00.html

1. OKTOBER 2019
EUGH-Entscheidung (C 673/17): Ein voreingestelltes Ankreuzkästchen bei Cookies, welches der Nutzer im Falle der Verweigerung abwählen muss, stellt keine zulässige Einwilligung in die Datenspeicherung dar.
http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=7511100

25. SEPTEMBER 2019
VwGH-Erkenntnis (Ra 2019/05/0078): Baubewilligungen und die zugrundeliegenden Baupläne enthalten auch personenbezogenen Daten, an denen ein schutzwürdiges Geheimhaltungsnteresse besteht.
https://www.ris.bka.gv.at/Dokumente/Vwgh/JWR_2019050078_20190925L08/JWR_2019050078_20190925L08.html





7. AUGUST 2019
DSB-Entscheidung (DSB-D123.737/0003-DSB/2019): Veröffentlichung der Adressen von Nachbarn, die zur Bauverhandlung eingeladen werden, verstößt gegen das Recht auf Geheimhaltung. Bei der Gemeinde handelt es sich um eine staatliche Behörde, die Verwendung von personenbezogenen Daten darf nur auf Grund des Gesetztes erfolgen. Eine solche gesetzliche Bestimmung lieg allerdings nicht vor.
https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20190807_DSB_D123_737_0003_DSB_2019_00/DSBT_20190807_DSB_D123_737_0003_DSB_2019_00.html

24. JULI 2019
OGH-Entscheidung (6Ob45/19i): Die Gewährung der Akteneinsicht (§ 219 ZPO) ist gleichzeitig als Verarbeitung von personenbezogenen Daten iSd Art. 4 Z 2 DSGVO zu qualifizieren. DSGVO ist dann anzuwenden, wenn Akteneinsicht die Person identifizierbare Informationen enthält.
HTTPS://WWW.RIS.BKA.GV.AT/DOKUMENT.WXE?ABFRAGE=JUSTIZ&DOKUMENTNUMMER=JJT_20190724_OGH0002_0060OB00045_19I0000_000

26. JUNI 2019
ArbG Lübeck (1 Ca 538/19): Die Veröffentlichung des Fotos vom Arbeitnehmer in sozialen Netzwerken, bedarf einer zusätzlichen Einwilligung.
Der Arbeitnehmer willigte nur in die Veröffentlichung seines Fotos auf der Homepage des Unternehmers. Von der Veröffentlichung auf Facebook wurde er nicht unterrichtet. ArbG sah einen Schadenersatzanspruch iHv 1000,- gerechtfertigt. Ein Urteil wurde nicht gefällt, da die Parteien sich auf einen Vergleich geeinigt haben.
https://www.juris.de/jportal/prev/KARE600058519

24. MAI 2019
BVwG-Entscheidung (W258 2205602-1): Bei Ausstellung der Kontoauszüge, die elektronisch (Online Banking) nicht mehr verfügbar sind, darf keine Gebühr erhoben werden. Im gegenteiligen Fall wird das Recht auf Auskunft nach Art. 15 DSGVO verletzt.
https://www.ris.bka.gv.at/Dokumente/Bvwg/BVWGT_20190524_W258_2205602_1_00/BVWGT_20190524_W258_2205602_1_00.html

16. APRIL 2019
DSB-Entscheidung (DSB-D213.679/0003-DSB/2018): Benützung der Sommerrodelbahn darf nicht von der Einwilligung in die Bildverarbeitung abhängig gemacht werden. Ohne Abgabe der Einwilligung kann die Sommerrodelbahn nicht benutzt werden, was ein Nachteil für den Betroffenen bedeutet. Das wiederum stellt eine unfreiwillige Einwilligung dar und verstößt gegen Art. 7 DSGVO.
https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20190416_DSB_D213_679_0003_DSB_2018_00/DSBT_20190416_DSB_D213_679_0003_DSB_2018_00.html

9. APRIL 2019
DSB-Entscheidung (DSB-D123.589/0002-DSB/2019): Weitergabe von personenbezogenen Daten für die Mängelbehebung aus einem Werkvertrag ist zulässig. Im Vertrag wurde vereinbart, dass die Leistungen teilweise oder zur Gänze von ausführenden Unternehmern erfüllt wird. Für die Behebung der Mängel war die Weitergabe der Daten (Name, Adresse, Telefonnummer) erforderlich und stellt eine zulässige Beschränkung des Rechts auf Geheimhaltung.
https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20190409_DSB_D123_589_0002_DSB_2019_00/DSBT_20190409_DSB_D123_589_0002_DSB_2019_00.html

19. MÄRZ 2019
VG Lüneburg (4 A 12/19): Die Verarbeitung der GPS Daten im Rahmen der ordnungsmäßigen betrieblichen Nutzung der Fahrzeuge ist nicht für die Durchführung des Beschäftigungsverhältnisses erforderlich. Bei wenigstes geduldeten Privatfahrten besteht kein pauschales Überwachungsbedürfnis.
http://www.rechtsprechung.niedersachsen.de/jportal/portal/page/bsndprod.psml?doc.id=MWRE190000986&st=null&showdoccase=1

26. FEBRUAR 2019
EDPB Stellungnahme 4/2019 gem Art. 64 DSGVO zur Verwaltungsvereinbarung bei Übermittlung personenbezogener Daten zwischen Finanzaufsichtsbehörden im Europäischen Wirtschaftsraum (EWR) und Finanzbehörden außerhalb der EWR.
https://edpb.europa.eu/sites/edpb/files/files/file1/2019-02-12-opinion_2019-4_art.60_esma_de.pdf

23. JÄNNER 2019
EDPB Stellungnahme 3/2019 Stellungnahme 3/2019 zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung /DSGVO) (Art. 70 Absatz 1 Buchstabe b).
https://edpb.europa.eu/our-work-tools/our-documents/avis-art-70/opinion-32019-concerning-questions-and-answers-interplay_de

20. DEZEMBER 2018
OGH-Entscheidung (6Ob131/18k): Die Verarbeitung personenbezogener Daten erfolgt dann nicht ausschließlich zu persönlichen oder familiären Zwecken, wenn die der Öffentlichkeit zur Verfügung gestellt werden. In diesem Fall greift die Ausnahme des Art. 2 Abs. 2 lit c nicht und Löschungsanspruch kann gerichtlich durchgesetzt werden.
https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20181220_OGH0002_0060OB00131_18K0000_000/JJT_20181220_OGH0002_0060OB00131_18K0000_000.html

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

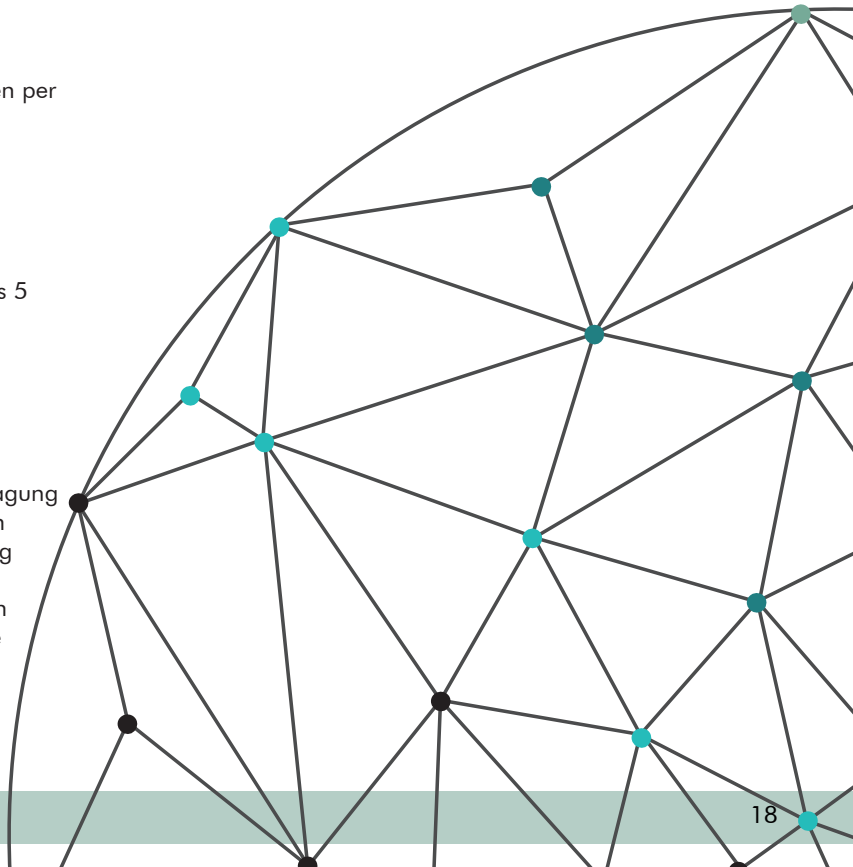
Geeignet für kleine und mittlere Unternehmen mit geringer Zahl an personenbezogenen Datensätzen und geringe Zahl von Verarbeitungen (max 3)

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-Assessments (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)

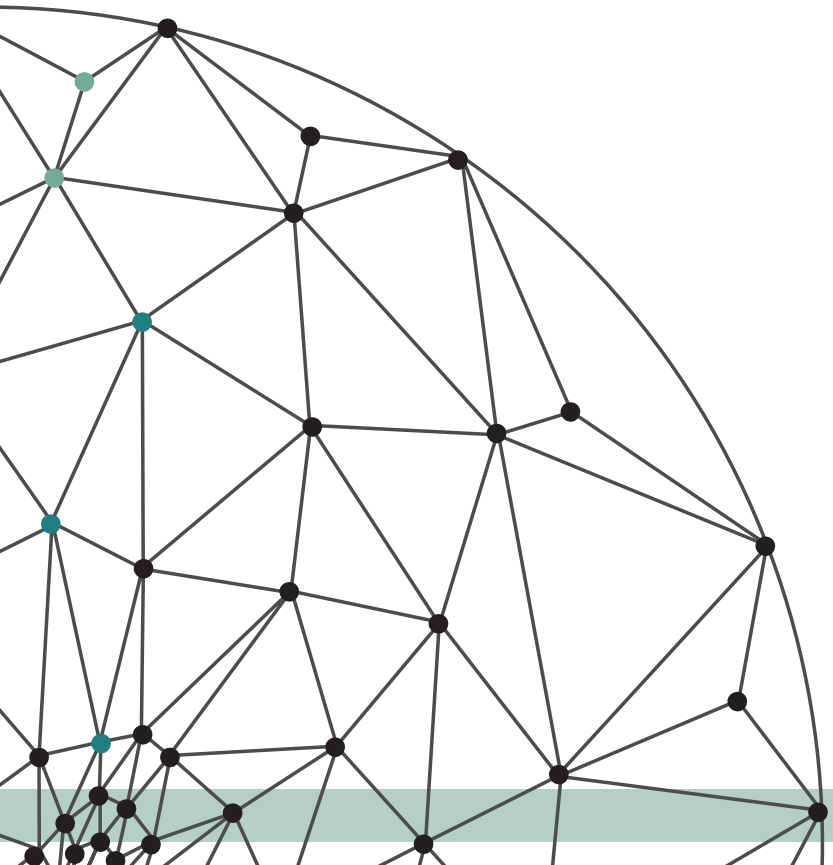


EXTERNER DATENSCHUTZBEAUFTRAGTER - FULL

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

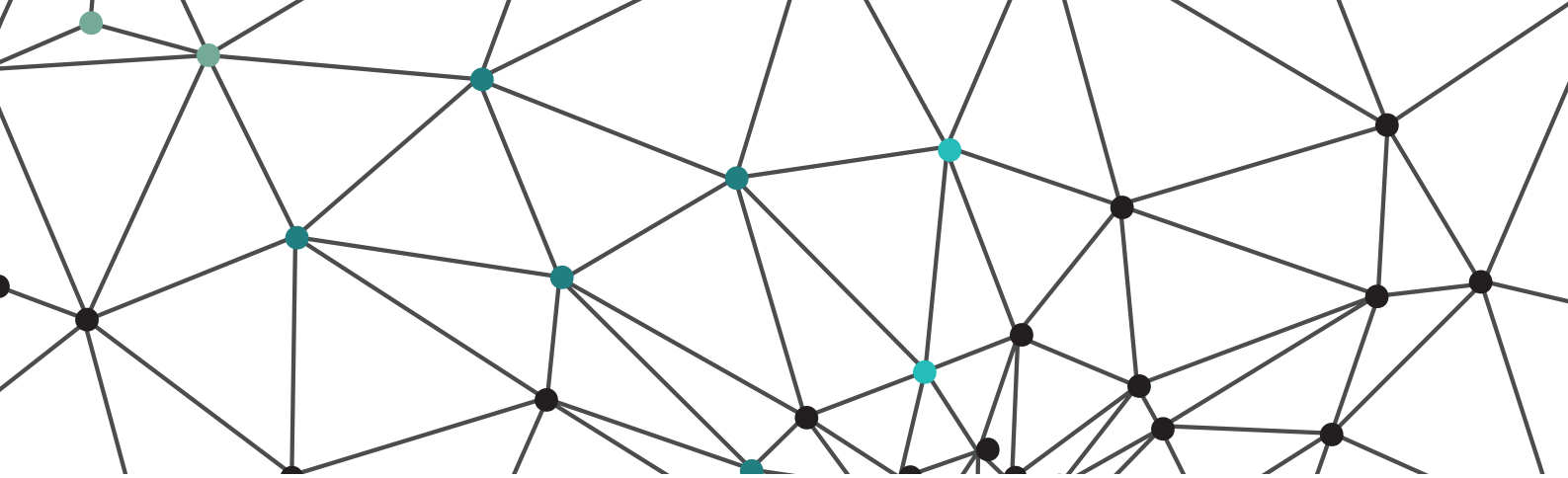
Servicebetrieb zur Abwicklung von Bestellungen und Verrechnung:
e-commerce monitoring GmbH, HG Wien FN 224536 a
http://www.e-monitoring.at

Bildnachweis:
S. 8, 11, 12 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 Komarow 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, 1020 Wien, Handelskai 388 (Eingang Wehlistr. 299/6/EG/621) (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.