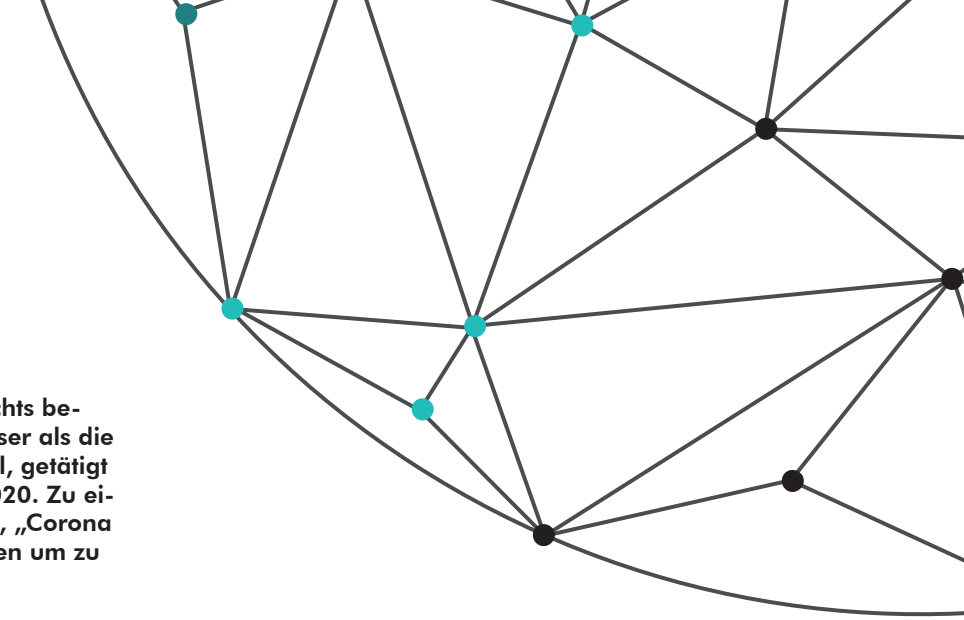
PRIVACY AUSTRIA TÄTIGKEITSBERICHT 2020/21

ARGE DATEN

http://www.argedaten.at/



EDITORIAL

„Corona ist eine demokratische Zumutung“ Nichts beschreibt das Top-Thema der Jahre 2020/21 besser als die Aussage der deutschen Bundeskanzlerin Merkel, getätigt bei ihrer Bilanz-Pressekonferenz im Sommer 2020. Zu einem Zeitpunkt, zu dem viele in Europa dachten, „Corona is over“. Heute wissen wir, Corona ist gekommen um zu bleiben.

Auch bei der ARGE DATEN ist Corona nicht spurlos vorüber gegangen. Die beliebten Datenschutzschulungen und unsere Jahrestagung 2020 mussten abgesagt werden, auch für 2021 sind keine Veranstaltungen geplant. Die Alternative „Online-Tutorials“ ist für uns keine Alternative, da unsere Tagungen und Schulungen vom regen Gedankenaustausch der Teilnehmer (auch in den Pausen) leben. Zahllose kniffelige Datenschutzfragen hätten wir nicht ohne vertrauliche Pausengespräche lösen können.

DATENSCHUTZ ABSEITS VON CORONA

Es gibt auch ein Leben außerhalb von Corona und so gab es auch im letzten Jahr einige wichtige Datenschutzentscheidungen. Unter anderem kippte der EuGH - wieder einmal - das Datenschutzabkommen „Privacy Shield“ zwischen EU und USA. Längst überfällig, hatten doch Experten schon bei der Verabschiedung 2016 die Vereinbarkeit mit europäischen Grundrechten bezweifelt.

Sie erinnern sich noch an unseren letzten „Aufreger des Jahres“? Mit 18 Mio. Euro erhielt die Post AG eine Rekord-Datenschutzstrafe weil sie sich als Austro-Google mit Weltanschauungsprofiling versuchte. Damals nicht rechtskräftig, jetzt vom BVwG aufgehoben, weil - diplomatisch formuliert - die Datenschutzbehörde pfuschte. Im Strafbescheid wurde nicht kenntlich gemacht, welche Organe der Post AG für den Datenmissbrauch tatsächlich verantwortlich wären.

Im Oktober 2020 wurde der verpflichtende elektronische Impfpass eingeführt. Damit wurde die Gesundheitsbürokratie erweitert, die „Freiwilligkeit“ von ELGA ausgehebelt und die persönliche Freiheit welche Gesundheitsleistungen in Anspruch genommen werden eingeschränkt. Der Impfpass ist ein entscheidender Schritt zum Impfzwang.

In einer richtungsweisenden Entscheidung hat das BVwG festgestellt, dass auch elektronische Signaturen einen geeigneten Identitätsnachweis darstellen. Damit ist - 20 Jahre nach Verabschiedung der EU-Signaturrichtlinie - das Digitale Zeitalter auch in Amtsstuben angekommen.

DAUERSTRESS CORONA

Datenschutz- und grundrechtlich verursachte Corona Dauerstress. Begonnen hat es im März 2020 mit unvorbereiteten und - wie sich nachträglich herausstellte - grundrechtswidrigen Ausgangsbeschränkungen. Damals, von März bis Mai 2020 hatte die Regierung von der Bevölkerung einen ungeheuren Vertrauensvorschuss. Auch rechtswidrige Beschränkungen wurden eingehalten in der Erwartung eines Plans, der hilft diese demokratische Zumutung zu bewältigen.

Die Erwartungen auf einen Corona-Plan wurden enttäuscht, zuerst im Mai 2020 und dann im Sommer 2020. Statt „wir sichern Gesundheitssystem und Bildungssystem koste es was es wolle“, wurden fehlerhafte Statistiken produziert, Sesselkreise folgten auf Ankündigungs-Pressekonferenzen und Geld wurde in Helikoptermanier planlos verstreut.

Statt Sicherung der Grundfreiheiten, wie Erwerbsfreiheit und Recht auf Familienleben spielte die Regierung mit dem Corona-Virus versteckerln. Ein bisserl von jeder Maßnahme wurde zu spät, zu kurz und zu inkonsequent probiert. Zusagen zu Förderungen, zu „Gratis“-Masken oder zu Gratis“-Tests wurden nicht oder nur eingeschränkt eingehalten.

Mindestens einmal in der Woche wurde das Licht am Ende des Tunnels für die nächsten Wochen angekündigt. Zumindest letzteres hören wir seit Beginn 2021 nicht mehr.

Wirklich chaotisch wurde es dann ab August 2020, als klar wurde, das Virus hat sich durch einen fehlenden Plan nicht vertreiben lassen.

- Aufhebung der Coronastrafen des Frühjahrs 2020 durch die Höchstgerichte

- Abstandsregeln in der Gastronomie, Schließungen im Handel, Schulschließungen, Demonstrationsverbote, alle Maßnahmen wurden von den Höchstgerichten als unbegründet, überschießend oder nicht geeignet aufgehoben.

- Statt Coronatests für alle, durfen sich im August 2020 nur Kroatien-Urlauber unbürokratisch testen lassen (es dauerte vier weitere Monate und 5.000 Coronatote mehr) bis das Testangebot ausgeweitet wurde.

- Ein Wiener Gastro-Gutschein sorgte im September für ordentliche Corona-Verbreitung (glücklich alle die keinen erhalten haben).

- Die Zettelwirtschaft mit persönlichen Daten bei Wirten sollte Corona verscheuchen, tatsächlich landen die Formulare im Eimer und das Virus bei den Besuchern (die ARGE DATEN warnte davor, der VfGH verurteilte des Projekt als rechtswidrig).

- Ab November 2020 brechen die sogenannten Contact-Tracing-Systeme der Bundesländer zusammen, die Aufklärungsquoten liegen unter 50%.

- Die Anmeldesysteme zum Coronatest würfelten im Dezember 2020 sensible Gesundheitsdaten durcheinander und verschickten sie an fremde Personen.

- Gratistests wurden nur an ELGA-Teilnehmer ausgegeben, ein weiterer Schritt zur Zwei-Klassen-Gesundheitsversorgung (ARGE DATEN berichtete)

- Ein seit Jänner 2021 andauerndes Impfchaos, verursacht durch falsche Einkaufspolitik der EU, einem Bundeskanzler der Verträge nicht sinnerfassend lesen kann und einem überforderten Gesundheitsminister, der es verabsäumt alternative Impfstoffquellen zu aktivieren.

- Ein Labor machte im Februar 2021 Testdaten von 80.000 Personen über das Internet zugänglich.

Warum Maßnahmen einhalten, wenn sie perspektivlos sind? Warum Vorschriften befolgen, wenn sie sowieso später aufgehoben werden?

Das Impfchaos erinnert an Karl Kraus' „Letzte Tage der Menschheit", erster Akt, Szene 11: Es ist erster Weltkrieg. Überraschenderweise kommt nach dem Herbst der Winter und für die Soldaten fehlen Wolldecken. Rasch werden welche beim deutschen Bündnisgenossen bestellt. Brauchen werden wir sie eh nicht, da die Epidemie, pardon der Krieg, schon vorher vorbei ist. Der Liefertermin ist da, es fehlen Zollpapiere. Der Finanzminister legt sich quer, der Kriegsminister bettelt um rasche Erledigung. Doch „Vurschrift is Vurschrift", es vergehen Wochen. Im Frühjahr ist es so weit. Doch die Decken waren unsachgemäß gelagert und sind verdorben. Aus zwei kaputten Decken wird eine neue genäht. Alles zu spät, zu teuer, ein Trost blieb. Die Soldaten brauchen die Decken eh' nicht mehr, wenn sie überhaupt noch leben sind ihre Füße längst abgestorben.

FREIHEIT, FREITESTEN, FREIGANG

Mit der Flut an chaotischen Gesetzen, Verordnungen, Erlässen, Ankündigungen, Interpretationen der Ankündigungen und Maßnahmen kommt es zu immer weiteren Einschränkungen unserer Freiheit.

Eric Blair, den meisten besser als George Orwell bekannt, warnte schon 1948 vor Newspeak. Jenes Sprachsystem, in der das Wort „frei" zwar noch existiert, aber nur mehr in der Kategorie als „frei von" gedacht wird. „Dieser Hund ist frei von Flöhen." oder in Corona-Newspeak übersetzt „Dieser Mensch ist frei von Corona, also freigetestet."

Freitesten war die erste Spielwiese der Regierung. Der geplante Corona-Ausweis (siehe unseren Aufreger des Jahres) ist der nächste Schritt.

Österreich befindet sich mit dem Ausweis-Projekt an einer gefährlichen Weggabelung. Maßnahmen wie der Corona-Ausweis verlassen den Grundrechtskonsens und haben zunehmend autoritäre Züge.

Geht dieser Ausweis durch, wo liegt die Grenze? Es gibt unzählige weitere Bedrohungen des Gesundheitssystems: sorglose Freizeitsportler, Colatrinker, Dauerraucher, Alkoholiker, Fettleibige, Couch-Potatos, alles voll mit Gefährdern der öffentlichen Gesundheit. Für jeden könnte ein Gesundheitsausweis erfunden werden. Teilnahme am gesellschaftlichen Leben ist dann nur jenen erlaubt, die ausreichend viele Plus-Punkte vorweisen können, ein Freigangs-Ausweis sozusagen.

Zu Redaktionsschluss scheiterte der Plan eine gesetzliche Grundlage zu schaffen vorerst am Votum des Bundesrates. Es mutet einigermaßen grotesk an, dass dieses Scheitern einer der massivsten Grundrechtseingriffe der - zufälligen Krankheit - einiger Bundesräte zu verdanken ist.

Auch auf EU-Ebene regt sich - nach einer Nachdenkphase - Widerstand gegen dieses Vorhaben. Ob der Corona-Ausweis bei Vorliegen des Druckexemplars in Kraft ist, kann die ARGE DATEN nicht beurteilen. Dass dieser Ausweis mittelfristig durch die Höchstgerichte als grundrechtswidrig aufgehoben wird ist jedoch ziemlich sicher.

Im übrigen bin ich der Meinung, dass die Regierung unverzüglich beginnen sollte die Pandemie ernst zu nehmen und einen wirkungsvollen Generalplan zur Bewältigung der Corona-Situation und der Regierungs-Krise vorlegen und umsetzen soll.

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

AUFREGER DES JAHRES

DER CORONA-AUSWEIS (VULGO „GRÜNER-PASS“)

Im Grunde ist alles rund um Corona ein Aufreger des Jahres, aus Datenschutzsicht sind es jedoch die Vorgänge rund um den Corona-Ausweis, euphemistisch umschrieben als „Grüner Pass“.

Der „Grüne Pass“ soll zentral Informationen zum Coronastatus einer Person speichern (Impfungen, Testungen und Genesungen). Abrufbar sind die Daten mittels Smartphone-App oder einem Zettel mit QR-Code. Der QR Code liefert Gesundheitsinformationen zu einer Person und soll europaweit in jedem Hotel, am Flughafen und sonstigen Einrichtungen gescannt und anerkannt werden. Die ausgelesenen Daten sollten auf das nötige Minimum beschränkt werden. Die Einsicht wird in die Identifizierung der Person, verwendeten Impfstoff, Chargenzahl, Datum und Ort der Impfung/Testung gewährt. Die Informationen über Impfungen und Testungen sind Gesundheitsdaten, auch die negativen Tests zählen, wie DSB (GZ 2021-0.101.211) es in ihrem Bescheid entschieden hat, zu Gesundheitsdaten und sind somit sensible Daten im Sinne von Art 9 DSGVO.

Damit sollen Reisen, die Teilhabe am gesellschaftlichen Leben wieder ermöglicht werden. Der Vorschlag wird vehement von Österreich verfolgt und in der EU propagiert. Zumindest einige EU-Tourismusnationen stehen dem Projekt positiv gegenüber.

Die Idee hört sich im ersten Augenblick verlockend an. Derartige Initiativen suggerieren Handlungsfähigkeit der Regierung, Datenschutz oder die Grundrechte werden „vorläufig“ hintenangestellt und auf „bessere“ Zeiten verschoben.

Was ist schlecht an einem Corona-Ausweis, der nachweist, dass vorgeschriebene Schutzmaßnahmen befolgt wurden oder zumindest eine Corona-Erkrankung heil überstanden wurde?

Datentechnisch ist das System nicht durchdacht und auch nicht praxistauglich. Wird der QR-Code einmal gescannt, dann kann der Status beliebig oft abgerufen werden. Der Scanner kann sich dadurch einen regelmäßigen Überblick über den Gesundheitsstatus einer Person verschaffen, auch ohne deren Einwilligung.

Gleichzeitig erfährt das zentrale System von wo aus der Scan stattfand und erhält damit einen genauen Einblick, wann sich wer wo aufgehalten hat.

Im Grunde ist der Ausweis eine Vorratsdatenspeicherung auf Gesundheitsebene. Zur Teilnahme am gesellschaftlichen Leben, Nutzung der Grundrechte, wie Reisefreiheit, Erwerbsfreiheit, Versammlungsfreiheit oder freie Religionsausübung müssen sich Bürger und Bürgerin freibeweisen. Sie müssen nachweisen „ungefährlich“ zu sein, damit ist Österreich mitten in der Alibigesellschaft. Ein Ansatz der zuletzt im Zusammenhang mit der Vorratsdatenspeicherung der Telefondaten und ihrer Nutzung zur Terrorbekämpfung kläglich gescheitert ist.

Schon 2014 hatten EuGH und VfGH festgehalten, dass ein voraussetzungsloses und flächendeckendes Erfassen des Kommunikationsverhaltens ein zu weitgehender Eingriff in die Grund- und Freiheitsrechte ist. Mit dem Corona-Ausweis würden Gesundheitsdaten voraussetzungslos erfasst und die Verwendung zu beliebigen Zwecken durch beliebige Personen erlaubt werden.

Um das Problem „Corona-Ausweis“ zu verstehen, muss die Bedeutung von Grund- und Freiheitsrechten in Erinnerung gerufen werden.

Die Grund- und Freiheitsrechte sind vorrangig Abwehrrechte gegen Übergriffe durch den Staat. Alle BürgerInnen haben Anspruch darauf, nicht in den Rechten auf Erwerb, Meinungsfreiheit, Privat- und Familienleben, Versammlungsfreiheit, Religionsfreiheit, Recht auf Bildung und zahlreichen anderen Rechten eingeschränkt zu werden. Im Gegensatz zu anderen Ländern gibt es in Österreich keinen einheitlichen Grundrechtskatalog, die Website https://grundrechte.at/ bietet jedoch einen guten Überblick über die verschiedenen Rechtsstellen zu den Grundrechten.

Der Staat hat alles zu unterlassen, diese Grundrechte zu gefährden. So darf keine Straßenverkehrsordnung geschaffen werden, in der jeder nach Belieben fahren (vulgo „rasen“) darf. Dies würde das Leben zahlreicher Verkehrsteilnehmer gefährden. Der Staat wäre Urheber dieser Gefährdung. Aus gutem Grund wurde daher ab einer gewissen Fahrzeugdichte die Rechtsfahrregel für Fahrzeuge erlassen. Aus genau demselben guten Grund gibt es dieses Rechtsbewegungsgebot für Fußgänger NICHT. Die grundrechtliche Gefährdung des Lebens durch zwei zusammenstoßende Fußgänger ist geringer, als der Grundrechtseingriff in die Bewegungsfreiheit.

Corona stellt unbestritten eine massive gesundheitliche Bedrohung dar. Unbestritten ist jedoch auch - abgesehen von einigen Verschwörungstheoretikern -, diese Bedrohung wurde nicht von der österreichischen Regierung in die Welt gesetzt. Damit fehlt ein unmittelbarer Grundrechtsanspruch gegen den Staat auf Corona-Abwehr.

Es besteht jedoch ein Anspruch, dass der Staat alle notwendigen Schritte setzt, damit trotz Gesundheitsbedrohung die BürgerInnen alle Grundrechte so weitgehend wie möglich wahrnehmen können.

Entgegen landläufiger Meinung gibt es kein Grundrecht auf Gesundheit, sehr wohl jedoch einen Anspruch, dass der Staat nicht unser Grundrecht auf (Zusammen-)Leben, unsere Erwerbsfreiheit, unsere Meinungs- und Versammlungsfreiheit, unser Privat- und Familienleben, unsere Religionsfreiheit, unser Recht auf Bildung gefährden darf.

Der „Corona-Ausweis“ muss daran gemessen werden. Dabei helfen drei Prüfschritte: Ist die geplante Maßnahme (a) geeignet, (b) erforderlich und (c) angemessen um einen bestimmten Zweck zu erfüllen?

Zusätzlich verlangt die DSGVO für die Verarbeitung persönlicher Daten einen klar definierten Zweck. Der Zweck des „Corona-Ausweises“ ist offenbar Menschen vor Corona-Ansteckung zu schützen. Ein durchaus vernünftiger Zweck, hält der Ausweis jedoch der Grundrechtsprüfung stand?

(A) EIGNUNG

Einen „Corona-Ausweis“ erhalten alle Personen, die getestet, geimpft oder corona-genesen sind. Art. 83 DSGVO zählt mögliche Pflichtverletzungen auf, diese Aufzählung ist demonstrativ und soll der Verdeutlichung dienen, ist aber nicht abschließend.

Gemäß bisheriger Studien liegt die Fehlerquote der derzeit verwendeten Tests zwischen 5-50%. Weiters werden Personen kurz nach Ansteckung - noch - nicht erkannt und Personen können sich unmittelbar nach dem Test anstecken. Damit reduzieren Tests zwar die Weiterverbreitung, verhindern sie nicht. Subjektiv erhöhen sie das Sicherheitsgefühl, es ist jedoch umstritten wie hoch ihre objektive Wirkung ist. Wäre sie signifikant hoch, dann dürfte es bei bestehenden Eintrittstests zu keiner Erhöhung der Ansteckungen kommen. Dies ist jedoch - leider - nicht der Fall.

Zu den Impfungen existieren erst vorläufig Ergebnisse. Laut der Mehrheit der Studien verhindert eine Impfung die Weiterverbreitung des Virus durch den Geimpften nicht, bestenfalls wird die Verbreitung verringert. Zusätzlich hat der weitaus überwiegende Teil der Impfwilligen gar keinen Zugang zur Impfung.

Bleiben noch die Corona-Genesenen. Nach bisherigen Erfahrungen geht von diesen Personen tatsächlich kein Ansteckungsrisiko aus. Es kann aber wohl nicht Strategie der Regierung sein, möglichst viele Ansteckungen zu erreichen. Da wäre der Corona-Ausweis sogar kontraproduktiv.

In Summe fehlt dem Corona-Ausweis die Eignung das angestrebte Ziel zu erreichen, die weiteren Prüfschritte könnten entfallen, sollen jedoch der Vollständigkeit halber dargestellt werden.

(B) ERFORDERLICH

Eine geeignete Maßnahme darf nur dann eingesetzt werden, wenn es keine Alternativen gibt, die zu geringeren Grundrechtseingriffen führt („Alternativlos").

Da der Corona-Ausweis nicht die Ansteckung verhindert, sondern bloß die Wahrscheinlichkeit reduziert, muss geprüft werden, welche anderen Maßnahmen ebenfalls die Wahrscheinlichkeit reduzieren. Möglicherweise sogar stärker reduzieren, als der Corona-Ausweis.

Es gibt zahlreiche alternative Maßnahmen:
- Abstandsregeln
- Aufenthalt im Freien
- geeignete Masken
- Raumlüftung, Desinfektionsmöglichkeiten
- vermeiden direkter Kontakte, wie Händeschütteln, ...
- verhindern von Kontakten mit potentiell infizierten Flächen

Jede dieser Maßnahmen bedeutet einen geringeren Grundrechts- und Datenschutzeingriff als der Corona-Ausweis. Gleichzeitig haben diese Maßnahmen den Vorteil direkt geprüft werden zu können und erlauben individuelle Variation, abhängig von der konkreten Gefährdungslage der beteiligten Personen.

Da es zum Corona-Ausweis Alternativen gibt, die zumindest gleichwertig sind, fehlt dem Ausweis die notwendige Erforderlichkeit.

(C) ANGEMESSEN

Selbst wenn argumentiert wird, der Ausweis sei eine nützliche zusätzliche Maßnahme zu anderen Corona-Maßnahmen und daher „alternativlos", muss die Angemessenheit bewertet werden.

Nicht angemessen ist eine Maßnahme, wenn sie trotz Eignung und Erforderlichkeit zu massiv in Grundrechte eingreift.

Im Fall des Corona-Ausweises ist das der Fall bei Personen, die aus gesundheitlichen Gründen oder mangels Verfügbarkeit an Impfstoff nicht geimpft werden können. Sie wären vom gesellschaftlichen Leben weitgehend ausgeschlossen. Sie könnten nicht spontan Reisen, Lokale oder Religionsstätten betreten, kulturellen Neigungen oder Sport nachgehen, pflegebedürftige Angehörige treffen oder einkaufen.

Weiters würde ein Corona-Ausweis zur Offenlegung sensibler Gesundheitsdaten gegenüber Laien verpflichten. Ein Eingriff, der durch die DSGVO ausgeschlossen ist.

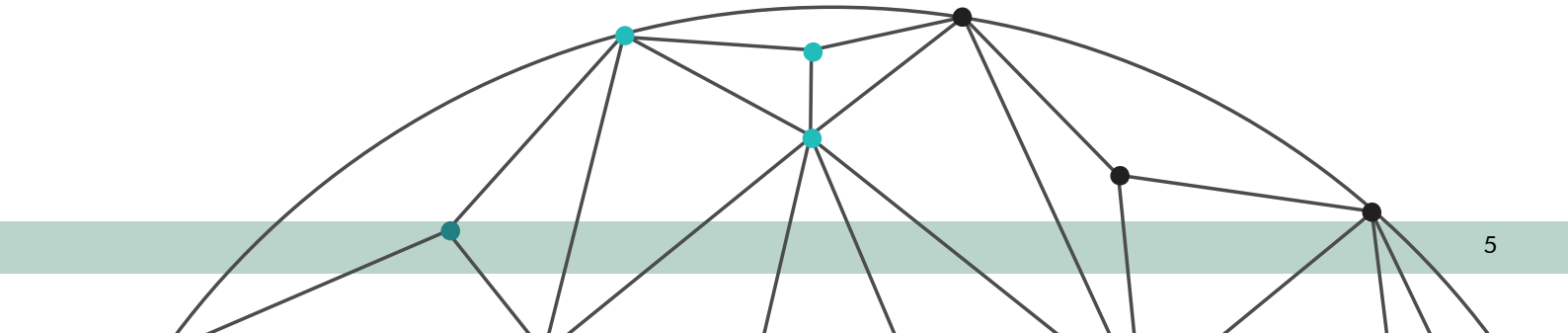
Schon aus diesen Gründen ist der Corona-Ausweis mit europäischen Grundrechten unvereinbar.

TÄTIGKEITSBERICHT ARGE DATEN 2020/21

Beispiele aus der Beratungspraxis der ARGE DATEN

- **Bonität:** Löschung der negativen Einträge gegenüber den Wirtschaftsauskunftsdiensten
- **Hausverwaltung**: Unaufgefordertes Anbringen von Namensschildern bei Hauseingang
- **Gesundheit:** Verarbeitung falscher medizinischer Diagnosen
- **KFZ:** Kennzeichenerfassung beim Kurzparken, Abstandmessung auf der Autobahn
- **Behörden:** Vorgehensweise beim Auskunftsbegehren
- **Bank:** Selbstauskunft über gespeicherte Daten, Widerrufsrecht
- **Privatleben:** Datenerfassung mittels Kameraüberwachung
- **Gesundheit:** Widerspruch bei den E-Rezepten, Informationen zum E-Impfpass
- **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
- **Verwaltung:** Weitergabe privater Handynummern durch Ladungsbrief
- **Gemeinde**: Müllplatznutzung mittels E-Card
- **Zeitung:** Veröffentlichung privater Adressen ohne Zustimmung des Betroffenen
- **Privatleben**: Einbau von Smart Metern

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



ANFRAGEN AUS DER PRAXIS

ARGE DATEN präsentiert eine Auswahl von Datenschutzanfragen aus dem letzten Jahr, die aus unserer Sicht im öffentlichen Interesse sind.

KENNZEICHENERFASSUNG MITTELS SCAN

ANFRAGE: Auf einem Fabrikgelände mit unterschiedlichen Startup Unternehmen werden Kennzeichen gescannt, obwohl auf der Homepage die Parkplätze als kostenlose Kurzparkplätze ausgeschrieben werden. Bei der Bezahlung am Automaten muss das Kennzeichen angegeben werden, erst dann wird die Parkgebühr errechnet. Bei der Zahlung im, auf dem Gelände befindlichen, Geschäft wird die Parkgebühr nach Angabe des Kennzeichens und dem Abgleich mit Kundendaten freigeschalten

ANTWORT: In einem ähnlichen Fall (DSB-D123.652/0001/2019) der automatischen Kennzeichenerfassung in der Parkgarage entschied die Datenschutzbehörde, dass die automatisierte Kennzeichenerfassung nicht unüblich ist. Das Interesse der Raschheit und Effizienz bei Abwicklung von Kurznutzungsverträgen muss dabei überwiegen. Die Daten dürfen nicht weiterverarbeitet und müssen nach der Abwicklung der Abrechnung gelöscht werden.

In dem geschilderten Fall ist fraglich, ob das gebotene Interesse überwiegt. Allein schon aus dem Grund, dass die Parkplätze laut der Homepage kostenlos angeboten werden, erübrigt sich die Abwicklung von Kurznutzungsverträgen.

Die Nennung der Kennzeichen und Abgleich mit den Kundendaten stellt keine freiwillige Einwilligung in die Datenverarbeitung dar. Da der Verbraucher ohne die Einwilligung schlechter gestellt wäre, sprich Parkgebühren zahlen müsste. Eine DSGVO-Konforme Verwendung der Kennzeichenerfassung ist für ARGE DATEN nicht erkennbar.

Wir empfehlen eine Beschwerde bei der Datenschutzbehörde einzureichen.

INHALTLICHE ANFORDERUNGEN AN DIE AUSKUNFT

ANFRAGE: Eine Internetseite verarbeitet personenbezogene Daten. Als Antwort auf das Auskuftsbegehren wird ein kurzes Mail zugeschickt, dass nur die Daten verarbeitet werden, die die Kundin eigenständig eingegeben hat.

ANTWORT: Die Antwort entspricht nicht den gesetzlichen Vorschriften. Die Auskunft nach Art 15 DSGVO muss auch dann erteilt werden, wenn keine persönlichen Daten verarbeitet wurden. Wird vom Verantwortlichen bestätigt, dass Daten über betroffene Personen verarbeitet werden, so besteht zudem das Recht auf folgende Auskünfte:

- Verarbeitungszwecke,
- Kategorie personenbezogener Daten, die verarbeitet werden,
- Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittstaaten,
- falls möglich, die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
- das Bestehen des Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchrechts gegen diese Verarbeitung,
- das Bestehen des Beschwerderechts bei einer Aufsichtsbehörde,
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling, aussagekräftige Information über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Bei unzureichender Auskunft empfehlen wir eine Beschwerde bei der Datenschutzbehörde einzureichen.

RECHTLICHE REGELUNG BEI VIDEOÜBERWACHUNG

ANFRAGE: Was muss beim Anbringen von Kameras beachtet werden und welche gesetzlichen Regelungen sind vorgesehen?

ANTWORT: Das DSG gestattet den Einsatz von Bildverarbeitungsanlagen (Videoüberwachungen) im privaten Bereich innerhalb bestimmter Grenzen.

Folgende Gründe können den Einsatz einer Videoüberwachung rechtfertigen:

- Schutz des Lebens von Personen,
- Schutz der Gesundheit und der körperlichen Unversehrtheit von Personen,
- Schutz des Eigentums (beispielsweise des Eigenheims).

In allen Fällen sind folgende Kriterien zur Bestimmung der Zulässigkeit heranzuziehen:

- die Videoüberwachung erfolgt zeitlich und örtlich nur im unbedingt erforderlichen Ausmaß.
- Ein Einbeziehen öffentlicher Verkehrsflächen (beispielsweise Gehsteig oder Straße) ist nur dann zulässig, wenn der Schutzzweck der Videoüberwachung sonst nicht erfüllt werden könnte (zum Beispiel Überwachung einer an einen Gehsteig grenzenden Fassade zum Schutz vor Sachbeschädigung im Ausmaß von maximal 50 Zentimetern). Nachbargrundstücke dürfen jedenfalls nicht gefilmt werden.
- die Videoüberwachung ist geeignet gekennzeichnet (durch Schilder, Aufkleber und dergleichen).
- die Aufnahmen werden in regelmäßigen Abständen überschrieben/gelöscht. Eine Speicherdauer von mehr als 72 Stunden muss verhältnismäßig sein und bedarf einer gesonderten Protokollierung (§ 13 Abs 3).
- eine Auswertung der Aufnahmen erfolgt nur im Anlassfall (zum Beispiel um festzustellen, wer eine Beschädigung durchgeführt hat).

• andere, gelindere Mittel würden sich als unzureichend erweisen (zum Beispiel Sperrsysteme, Sicherungssysteme und dergleichen).

Als Rechtsgrundlage für Videoüberwachungen im privaten Bereich kommt im Regelfall Art. 6 Abs. 1 lit. f DSGVO (berechtigte Interessen des Verantwortlichen), wie er in der Rechtsprechung des EuGH (C-708/18) ausgelegt wird, in Betracht. In bestimmten Fällen kann eine Videoüberwachung auch auf Art. 6 Abs. 1 lit. a DSGVO (Einwilligung der betroffenen Personen) gestützt werden.

Folgende Punkte sind zu beachten:

• Die Beurteilung, ob eine Videoüberwachung als zulässig angesehen werden kann, obliegt dem Verantwortlichen. Diese Prüfung muss vor der Inbetriebnahme der Anlage erfolgen. Gleiches gilt für die Frage, ob in einem konkreten Fall eine Datenschutz-Folgenabschätzung durchzuführen ist oder nicht. Die Datenschutzbehörde nimmt jedenfalls keine diesbezüglichen Vorabbeurteilungen vor.

• Es besteht keine Meldepflicht derartiger Anlagen an die Datenschutzbehörde.

VERSICHERUNG WIRBT FÜR ANDERE PRODUKTE

ANFRAGE: Eine private Unfallversicherung schickt dem Kunden Werbung von einer anderen Versicherungssparte ohne Einwilligung zu. Auf die Nachfrage des Kunden berief sich der Datenschutzbeauftragte der privaten Unfallversicherung auf berechtigtes Interesse, welches die Übermittlung von Werbung rechtfertigt.

ANTWORT: Bei den Kontaktdaten handelt es sich um persönliche Daten. Grundsätzlich muss der Betroffene in die Verarbeitung seiner persönlichen Daten einwilligen. Die DSGVO führt auch anderen Varianten auf, bei denen die Verarbeitung bzw. Weitergabe ohne Einwilligung zulässig ist. Die Weitergabe könnte zum Beispiel für die Vertragserfüllung erforderlich sein (Art 6 Abs. 1 lit b DSGVO) oder berechtigtes Interesse an der Weitergabe von Daten bestehen (Art 6 Abs. 1 lit f DSGVO). Dazu gehören auch wirtschaftliche Interessen, wie an der Erzielung des Gewinns, Kostensenkung, Optimierung der Dienste usw. Bei der Interessenabwägung kommt es auf die Art der Daten, den Zweck der Datenweitergabe und die möglichen Risiken für den Betroffenen an.

Wenn die Adressdaten an andere Versicherungen weiterverkauft werden um gezielte Werbung zu betreiben, wird die Interessenabwägung negativ ausfallen. Bleiben die Daten innerhalb eigener Versicherung und der Kunde bekommt nur Werbung für andere Versicherungsarten, liegt ein berechtigtes Interesse vor.

EXEKUTOR BEFRAGT NACHBARN

ANFRAGE: Der Exekutor befragt die Nachbarn über den Schuldner. Grundsätzlich wird die Frage zu seiner Anwesenheit an der Wohnadresse gestellt.

Im Gespräch erzählen die Nachbarn zusätzlich wer noch mit in der Wohnung wohnt und dass der Schuldner noch einen anderen Wohnsitzt hat.

ANTWORT: Der Exekutor darf nach verbreiteter Meinung grundsätzlich die Nachbarn kontaktieren und Fragen stellen. Die Fragen wann der Nachbar zuhause anzutreffen ist, sind zulässig. Wenn die Nachbarn von selbst mehr erzählen, darf es dem Exekutor nicht vorgehalten werden, weil er diese Informationen ohne sein Zutun erlangt hat. Deswegen kommt es in Ihrem Fall drauf an, was und wie die Nachbarn gefragt wurden.

Bei Exekutionen ist nicht die DSGVO, sondern die Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr ((EG) Nr. 45/2001) anwendbar. Die Zuständigkeit der Datenschutzbehörde bleibt unberührt.

Die betroffene Person kann sich an die Datenschutzbehörde wenden um die Verletzung Ihres Rechts auf Datenschutz festzustellen, allerdingst muss die betroffene Person nachweisen, dass der Exekutor die Nachbarn gezielt ausgefragt hat.

LÖSCHUNG POSITIVER BEWERTUNGEN AUF GOOGLE

ANFRAGE: Es sollen die positiven Bewertungen von Google gelöscht werden. Dabei handelt es sich um ein Unternehmen, welches bei der WKO eingetragen wird.

ANTWORT: Für Unternehmen besteht kein Recht auf Geheimhaltung nach DSGVO. Selbst negative Bewertungen müssen nicht gelöscht werden, wenn diese sachlich begründet sind. Bei sachlich unbegründeten Bewertungen besteht ein Unterlassungsanspruch nach der allgemeinen Bestimmungen des ABGB.

In einem Fall (LG Hamburg, 12.01.2018, 324 O 63/17) mit 1-Stern-Bewertung ohne Text verpflichte das Landesgericht Hamburg Google zur Prüfpflicht und anschließender Löschung der Rezension. Diese 1-Stern-Bewertung ohne Begründungstext verletzt die Persönlichkeitsrechte des Unternehmers.

Da es sich im oben genannten Fall um positive Bewertungen handelt, sieht die ARGE DATEN keine Erfolgschancen auf Löschung.

KOSTENLOSER IMPRESSUM- UND DATENSCHUTZGENERATOR

ANFRAGE: Zahlreiche Internetseiten bieten einen kostenlosen Impressum-Generator an. Dafür muss man individuelle Daten des Unternehmens eingeben und bekommt ein vorgefertigtes Impressum und die Datenschutzbestimmungen per E-Mail geschickt. Diese müssen laut AGBs zur Gänze übernommen werden, sollten eine Passage herausgenommen werden, können Schadenersatzansprüche entstehen.

Sollen Links und Verweise auf den Anbieter unerwünscht sein, besteht die Möglichkeit eine kostenpflichtige Version zu bekommen. Der um Rat Ansuchende entschied sich für die kostenlose Version, übernahm jedoch nicht alle eingebauten Textpassagen mit Links. Mehrere Wochen später machte der Anbieter seine Schadersatzansprüche geltend.

ANTWORT: Der Anbieter des Impressum-Generators verdient Geld in dem er Werbung mit den eingebauten Links in den generierten Texten macht. Beim Eingeben und Absenden der individuellen Daten zum Impressum-Generator wird ein Vertrag abgeschlossen. Die Verarbeitung der Daten durch den Anbieter erfolgt gem Art 6 Abs 1 lit b DSGVO und ist zulässig. Der Anbieter des Impressum-Generators überprüft die Vollständigkeit der generierten Texte in dem er mittels Suchmaschine nach im Text eingebauten typische Passagen sucht. Das stellt keine Verletzung der DSGVO dar, weil die Verarbeitung ein Teil des Vertrages ist.

Im ersten Augenblick sieht die Vertragskonstruktion wie eine unzulässige Koppelung aus, die Einwilligung würde dann als unfreiwillig erteilt (iSv Art 7 Abs 4 DSGVO) gelten. Eine unzulässige Koppelung liegt dann vor, wenn die Verarbeitung personenbezogener Daten unabhängig von Vertragserfüllung oder Dienstleistungserbringung ist.

Das Geschäftsmodell von kostenlos im Internet angebotenen Diensten wird durch in DSGVO geregeltes Koppelungsverbot in Frage gestellt. Es werden Waren und Dienstleitungen für jeden Nutzer kostenlos angeboten, im Gegenzug müssen die Nutzer der Verarbeitung ihrer personenbezogenen Daten zu Werbezwecken zustimmen (zB ein kostenloser Internet-Dienst, der sich durch personenbezogene Werbung finanziert).

Allerdings ist zu berücksichtigen, dass die datenschutzrechtliche Einwilligung und die Erbringung des Dienstes nicht notwendigerweise in einem rechtlichen, jedenfalls in einem wirtschaftlichen Austauschverhältnis stehen, sodass die Erteilung der Einwilligung erst die wirtschaftlichen Voraussetzungen für das unentgeltliche Zurverfügungstellen der Waren oder Dienstleistung schafft. Insofern kann in derartigen Fällen argumentiert werden, dass die Einwilligung für die Erfüllung des Vertrages (wirtschaftlich) erforderlich ist und daher eine wirksame Einwilligung vorliegt.

Etwas anderes gilt, wenn die betroffene Person für die Waren oder Dienstleistungen sehr wohl ein angemessenes Entgelt bezahlt und daher die Einwilligung keine Voraussetzung für die Wirtschaftlichkeit der Leistungserbringung ist.

Aus Sicht der ARGE DATEN wurde durch die nur teilweise Übernahme des generierten Textes das Urheberrecht verletzt. Im ersten Augenblick könnte man Impressum und Datenschutzbestimmungen für Rechtstexte ohne Schutzanspruch halten. Es sind unter Urheberrecht fallende selbst verfasste Texte, deren Grundlage Rechtsvorschriften sind. Dazu hat OGH bereits 2013 entschieden (4Ob236/12b).

Abschließend ist festzuhalten, dass Impressum- und Datenschutztexte keine Gesetzestexte sind. Für die Nutzung dieser Texte wird ein Vertrag abgeschlossen, die Verarbeitung der Daten erfolgt aufgrund vertraglicher Pflichten. Dafür Kosten zu verlangen oder die Verwendung an die Regeln zu binden ist nicht rechtswidrig.

AKTUELLE DATENSCHUTZTHEMEN UND -ENTSCHEIDUNGEN

BVWG: ELEKTRONISCHE SIGNATUR IST AUSREICHENDER IDENTITÄTSNACHWEIS

In der Entscheidung (W214 2228346-1/16E) vom 27.5.2020 entschied das Verwaltungsgericht über die Zulässigkeit vom Identitätsnachweis beim Auskunftsbegehren nach Art 15 DSGVO.

OHNE ZUSÄTZLICHEN IDENTITÄTSNACHWEIS BLEIBT MAGISTRAT UNTÄTIG

Anlass gab die Beschwerde bei der Datenschutzbehörde, weil das Magistrat dem Auskunftsbegehren mit der Begründung nicht nachkam, der Betroffene habe, auch nach Verstreichen der Frist, keinen geeigneten Identitätsnachweis (Art 12 Abs 6 DSGVO) zur Verfügung gestellt. Die Daten (Name, Wohn-, E-Mailadresse) des Betroffenen waren vor dem Ansuchen bereits in der Datenbank des Magistrats eingespeichert. Zudem gab es davor schon mehrmals einen E-Mail-Verkehr mit dem Betroffenen wegen einer anderen Angelegenheit. Das E-Mail mit dem Ansuchen einer Auskunft wurde mittels einer elektronischen Signatur verschickt, die eine Unterschrift ersetzt, zusätzlich wurde die neue und ehemalige Wohnadresse angeführt. Die Datenschutzbehörde stellte die Verletzung des Rechts auf Auskunft fest und gab der Beschwerde des Betroffenen statt. Das Magistrat legte eine Bescheidbeschwerde gegen die Entscheidung der Datenschutzbehörde ein.

Das Problem war dabei die qualifizierte elektronische Signatur. Das Magistrat hielt die elektronische Signatur als Ersatz für den Identitätsnachweis für unzureichend und unzulässig, da lediglich die Unterschrift ersetzt wird.

Das BVwG hielt zunächst fest, dass der Identitätsnachweis nicht „blind" verlangt werden kann, sondern nur in dem Fall, wenn die Identität auf eine andere Weise nicht festgestellt werden kann oder begründete Zweifel an dieser bestehen. Der Beschwerdeführer (Magistrat) hat zu keinem Zeitpunkt die Zweifel an der Identität angeführt. Durch die aktive Kommunikation per E-Mail mit dem Betroffenen, sowie die Versendung eines eingeschriebenen Briefes an die, wie im E-Mail angegeben, Wohnadresse war die Identität leicht feststellbar.

BEI SIGNATURAUSSTELLUNG WIRD IDENTITÄT BEREITS GEPRÜFT

Aus Sicht des BVwG stellt die elektronische Signatur ein geeignetes Mittel zum Identitätsnachweis. Bereits bei der Ausstellung von der Signatur wurde die Identität des Betroffenen vom Vertrauensdienstanbieter festgestellt, es gab auch keine Indizien, dass die Ausstellung rechtswidrig vorgenommen wurde. Somit weist die elektronische Signatur eine feste Personenbindung auf.

Abschließend ist festzuhalten, dass der Identitätsnachweis nur dann erforderlich ist, wenn berechtigte Zweifel bestehen und die Identität auf keine andere Weise festgestellt werden kann. Wenn die Kontaktdaten davor bekannt waren und eine längere Korrespondenz nachwiesen werden kann, besteht kein Grund für gesonderten Identitätsnachweis.

Die elektronische Signatur ersetzt den Identitätsnachweis, weil die Identität durch den Vertrauensdient überprüft wurde.

Im vorliegendem Fall hätte das Magistrat auch ohne elektronische Signatur die Auskunft erteilen müssen, weil bereits eine aktive Kommunikation mit dem Betroffenen vorlag.

ALLES RUND UM COOKIES

Cookies sind Textinformationen, die beim Anklicken einer Seite auf dem Computer des Nutzers gespeichert werden. Sie dienen der späteren Identifizierung der Nutzer und der Anpassung der Webseite. Beim erneuten Aufrufen der jeweiligen Internetseite werden Informationen über Themen und Produkte genutzt, die bereits beim vorherigen Besuch aufgerufen wurden. Die Cookies werden in vielen Bereichen eingesetzt und reichen von Online-Shops, Suchmaschinen und sozialen Netzwerken bis hin zu zielgerichteter personalisierter Werbung. In der Praxis werden die Cookies in vier Kategorien unterteilt: funktionale Cookies, Analyse-Cookies und Werbe-Cookies, Cookies Dritter.

EINHEITLICHE REGELUNG STEHT NOCH AUS

Regelungen zur Datenverarbeitung finden sich in Art. 95 DSGVO, Richtlinie 2002/58/EG („ePrivacy-Richtlinie"), Richtlinie 2009/136/EG („Cookie-Richtlinie") und Telekommunikationsgesetz. Von der EU geplante neue ePrivacy-Verordnung soll die alte ePrivacy-RL ersetzen. Wann genau diese in Kraft tritt ist noch nicht bekannt. Die Datenschutz-Compliance von Webseiten richten sich maßgeblich nach DSGVO, die jedoch keine spezielle Regelung für Webseiten enthält.

EINWILLIGUNG NUR DURCH AKTIVE HANDLUNG MÖGLICH

Der Einsatz von bestimmten Cookies (va Analyse- und Werbecookies) ist nur zulässig, wenn der Teilnehmer seine Einwilligung dazu erteilt hat. Da der Wortlaut der Richtlinie relativ schwammig formuliert ist, entschied sich Österreich für eine aktive Handlung (Opt-In) des Nutzers. Der Teilnehmer ist über die Nutzungsmöglichkeiten in den Verzeichnissen eingebetteten Suchfunktionen zu informieren. Jedenfalls muss der Nutzer unmissverständlich darüber in Kenntnis gesetzt werden, mit welcher Handlung er in die Cookies-Verwendung einwilligen kann. Diese Information muss solange auf der Webseite zu sehen sein, bis der Nutzer seine Einwilligung erteilt hat. Keine gültige Zustimmung liegt dann vor, wenn der Nutzer ohne aktive Einwilligung auf der Startseite verbleibt. Das Auskunftsrecht nach dem Datenschutzgesetz und der DSGVO bleibt unberührt.

EUGH: KEINE EINWILLIGUNG DURCH VORANGEKREUZTES KÄSTCHEN

In der Entscheidung (C-673/17) hat der EuGH über die Gestaltung von Cookies entschieden. Der Anlass für die Entscheidung war der Rechtsstreit zwischen Verbraucherzentrale Bundesverband e. V. und Planet49 GmbH (Anbieter für Online-Gewinnspiele).

Unter anderem wegen der Speicherung von Informationen auf dem Endgerät und dem Zugang zu den gespeicherten Daten.

Nach EuGH liegt keine wirksame Einwilligung vor, wenn die Speicherung von Informationen oder der Zugriff auf die Informationen, die bereits im Endgerät des Nutzers gespeichert sind, durch ein voreingestelltes Ankreuzkästchen erlaubt wird, welches der Nutzer zur Verweigerung seiner Einwilligung abwählen muss.

Im Erw 32 zur DSGVO wird eine aktive Einwilligung vorgesehen, was u.a durch Anklicken eines Kästchens beim Besuchen einer Internetseite zum Ausdruck kommen könnte. Dagegen wird in diesem Erwägungsgrund ausdrücklich ausgeschlossen, dass „Stillschweigen, bereits angekreuztes Kästchen oder Untätigkeit" eine Einwilligung darstellen.

Dabei ist es ohne Bedeutung, ob es bei der Speicherung von Informationen um personenbezogene Daten geht oder nicht. Damit soll jeder Eingriff in die Privatsphäre der Nutzer geschützt werden. Nach Erw 24 der e-Privacy-Richtlinie sind die in Nutzerendgeräten gespeicherte Informationen Teil der Privatsphäre der Nutzer. Dieser Schutz erstreckt sich auf alle in solchen Endgeräten gespeicherte Informationen, unabhängig davon, ob es sich um personenbezogene Daten handelt, die ohne Wissen der Nutzer in deren Endgeräte eindringen.

WEITERSURFEN IST AKTIVE HANDLUNG

Viele Online-Zeitungen setzen Cookies dann, wenn man ohne „Annehmen" zu klicken auf der Seite surft. In diesem Fall wird aktive Handlung angenommen. Problematisch ist oft, dass es keine Entscheidungsmöglichkeit gibt in welche Cookies eingewilligt wird.

KEINE UNVERHÄLTNISMÄSSIGKEIT BEIM ABO-ABSCHLUSS

Dazu hat sich die österreichische Datenschutzbehörde mit Beschluss von 30.11.2018 (DSB-D122.931/0003-DSB/2018) geäußert. Grundsätzlich hat die Einwilligung nach Art. 7 DSGVO freiwillig zu erfolgen und darf nicht an einen Vertrag gekoppelt werden. Unfreiwilligkeit liegt dann vor, wenn bei Nichtabgabe von Einwilligung ein Nachteil zu erwarten sei. Aus der Sicht der DSB kann der Nutzer die Zustimmung in die Cookies durch Abschluss eines kostenpflichtigen Abonnements umgehen. Das kostenpflichtige Angebot in diesem Fall betrug 6 Euro und war aus der Sicht der Behörde keine unverhältnismäßig teure Alternative. Sonst kann der Nutzer immer noch auf andere Internetportale ausweichen und auf alternatives Informationsangebot zurückgreifen.

Ähnlich sieht es auch die Datenschutzbehörde in Niederlande, der nach ist der Zwang nicht gegeben, wenn anstatt der Cookie-Einwilligung eine kostenlose oder kostenpflichtige Alternative angeboten wird.

Fazit: dem Nutzer muss kein kostenloser Zugang ohne eine Tracking-Einstellung angeboten werden.

GOOGLE WILL COOKIES ABSCHAFFEN

Google kündigte bereits 2019 an die Cookies im eigenen Browser nicht mehr zulassen zu wollen. Stattdessen soll eine „Privacy Sandbox" her, dabei werden die Nutzer nicht mehr einzeln analysiert, sondern in Gruppen unterteilt. Die Rückführung auf Individuen wäre dann nicht mehr möglich. Die personalisierte Werbung wäre dann auf die Gruppe angepasst.

Viele Anbieter schlagen andere Lösungen wie Log-in-IDs, Persistent Identifizierer, oder kontextuelles Targeting. Auf welches „Pferd" die Vermarkter und Werbeagenturen setzen sollen, lässt sich schwer sagen. Erst durchs Ausprobieren wird klar, welche Lösung die richtige ist.

Mit 40 Prozent der Marktanteile bei genutzten Internetbrowser kann es Google sich leisten neue Regeln aufzustellen und die anderen Anbieter dazu bringen auf den cookiefreien Zug aufzusteigen. Damit wird die Monopolstellung des Internetriesen nochmal befestigt.

Fraglich ist ob Google wirklich mit guten Absichten handelt und den Nutzern mehr Privatsphäre lassen möchte oder doch eine neue Strategie entwickelt um noch besseres Tracking zu betreiben. Schließlich sind die mit Cookies gesammelte Daten Goldwert, die Tatsache erweckt große Zweifel, dass Google einfach so darauf verzichten wird.

Ein weiterer Ansporn die Cookies abzuschaffen wäre die Vermeidung von Strafen durch die europäischen Datenschutzbehörden. Die letzte Strafe von 100 Millionen flatterte erst Ende des Jahres ins Haus. Die französische Datenschutzbehörde CNIL nahm die Setzung von Cookies durch Google genauer unter die Lupe und fand heraus, dass Cookies ohne Einwilligung der Nutzer gesetzt wurden.

Bei einem Jahresumsatz von circa 28 Milliarden Dollar können Strafen in dieser Höhe leicht verkraften.

ARTEN VON COOKIES

Der Europäische Datenschutzausschuss (früher Artikel-29-Datenschutzgruppe) hat eine Kategorisierung nach unterschiedlichen Zwecken vorgenommen :

- User-Input-Cookies: dabei handelt es sich um Session-Cookies, die dazu verwendet werden, die Eingaben der User auf der Webseite nachzuvollziehen und bedürfen keiner Zustimmung.
- Authentifizierung-Cookies: dienen der Identifizierung des Users, beim Einloggen auf der Webseite bekommt man den Zugang zu seinen Inhalten. Die Zustimmung ist nicht erforderlich, solange es sich um ein permanentes Login handelt.
- Security-Cookies: helfen dabei Datensicherheit auf der Webseite zu erhöhen und insbesondere das Login-System vor Missbrauch zu schützen. Die Zustimmung ist nicht erforderlich.
- Multimedia-Player-Cookies: speichern technische Daten, die das Abspielen von Videos oder Audios auf der Webseite ermöglichen. Die Zustimmung ist nicht erforderlich.
- UI-Customization-in-Cookies: speichern die bevorzugte Einstellung des Users, wie Sprach- und Sucheinstellungen. Die Zustimmung ist nicht erforderlich.
- Sozial-Plug-in-Cookies: bei sozialen Netzwerken werden die Cookies unterteilt in solche, die das Teilen von Inhalten ermöglichen und solche die das Verhalten der User im Internet speichern. Die Zustimmung für die ersten sind nicht erforderlich, solange nur die Daten von Usern verarbeitet werden, die in das soziale Netzwerkt eingeloggt sind. Für die zweiten ist die Einwilligung erforderlich.
- Werbe-Cookies: Die Werbung auf der Webseite, die durch Einbringung der Inhalte Dritter ermöglicht wird, bedarf der User-Einwilligung, welche vom jeweiligen Werbenden eingeholt wird.
- Analyse-Cookies: ermöglichen den Werbebetreibenden die Analysen eigener Seiten um dadurch die Inhalte zu verbessern. Die Zustimmung ist erforderlich.

ELEKTRONISCHER IMPFPASS

Seit 8. Oktober 2020 sind Änderungen im Gesundheitstelematikgesetz 2012 in Kraft. Neu dazugekommen sind die Regelungen zum elektronischen Impfpass. Zusätzlich wurde eine eHealth-Verordnung durch Bundesminister für Soziales, Gesundheit, Pflege und Konsumentenschutz verabschiedet, welche nähere Vorgaben zur Anwendung trifft.

Das Ziel der Gesetzesänderung ist die Optimierung der Impfversorgung der Bevölkerung sowie die Verfügbarkeit digitaler Impfinformationen für dir Steuerung des öffentlichen Gesundheitswesens. Dafür wurde ein zentrales Impfregister eingerichtet, in dem alle Dokumentationen zu durchgeführten Impfungen zusammengefasst werden.

VERARBEITUNG GROSSER MENGEN AN DATEN KÖNNTEN ANGEFÜHRTEM ZIEL WIDERSPRECHEN

Wenn man einen Blick ins Gesetz wirft, merkt man schnell welche Mengen an Daten gespeichert werden. Die Angaben zum Impfstoff, Zeitangaben der verabreichten Impfung und dem Empfänger der Impfung sind sehr präzise. Auch die impfende Gesundheitseinrichtung muss Namen, Rolle und Berufsadresse angeben. Automatisch stellt sich die Frage ob die Verarbeitung dieser Menge, unter anderem auch sensibler Daten dem im Gesetz angeführten Ziel entspricht. Für die Optimierung der Impfrate hätten auch weniger Angaben gereicht, damit man sehen kann wie die Impfrate ist.

KEINE OPT-OUT MÖGLICHKEIT

Sorgen bereitet auch die fehlende Opt-Out-Möglichkeit. Weder der Bertoffene noch der Gesundheitsanbieter kann die bereits eingetragenen Daten löschen. Erst 10 Jahre nach Strebedatum sind die Daten zu löschen. Alle neu gemachten Impfungen müssen verpflichtend eingetragen werden, die zuvor gemachten können nachgetragen werden, sind jedoch entsprechend zu vermerken. Die betroffenen Personen können gem Art 15 DSGVO die Auskunft über die im zentralen Register gespeicherten Daten verlangen.

POSITIVE ASPEKTE DES REGISTERS?

Grundsätzlich kann das Impfregister sich positiv auswirken und das Leben erleichtern. Die Impfpässe aus Papier gehen verloren oder werden zuhause vergessen. Bei der digitalen Erfassung kann der Arzt Einsicht nehmen und dem Patienten besser beratend zur Seite zu stehen. Dieses Ziel wäre auch durch einen freiwilligen elektronischen Impfpass erreichbar gewesen. Viele BürgerInnen sind sehr wohl imstande einen Papier-Impfpass sicher aufzubewahren.

POTENZIELLE DISKRIMINIERUNG UND GRUNDRECHTSVERLETZUNG MÖGLICH

Durch die fehlenden Austrittsmöglichkeiten bekommt man genauen Einblick über das Impfverhalten einzelner Personen. Es ist denkbar und angesichts des geplanten Corona-Ausweises erkennbar, dass Personen, die sich nicht impfen lassen, Nachteile haben. Da es viele Gründe gibt warum man nicht geimpft ist, kann es diskriminierend sein und die Grundrechte einzelner Personen einschränken.

Vor allem von denjenigen, die sich aus gesundheitlichen Gründen nicht impfen lassen können. Auch grundsätzliche Impfbefürworter werden aus Sorge um eigene Daten auf die Impfung verzichten oder sich außerhalb von Österreich impfen lassen, was genau den gegenteiligen Effekt hervorrufen wird.

10 MILLIONEN EURO STRAFE FÜR „GRINDR“

Die norwegische Datenschutzbehörde fällte am 24. Jänner 2021 eine Entscheidung über umgerechnet 10 Millionen Euro für die Dating App Grindr. Der Grund für eine so hohe Strafe war die rechtswidrige Weitergabe von sensiblen personenbezogenen Daten. Die Beschwerde wurde vom österreichischen Verein noyb gemeinsam mit dem norwegischen Verbraucherrat Anfang letzten Jahres eingereicht.

NUTZUNG DER APP NUR MIT ZUSTIMMUNG IN DIE DATENWEITERGABE MÖGLICH

Bei Grindr handelt es sich um ein soziales Netzwerk, welches auf schwule, bi- und transsexuelle Männer ausgerichtete ist. Die Daten über die Nutzung dieser App sowie Informationen von welchen Standorten aus auf die Daten zugegriffen wird, hat Grindr an hunderte Werbepartner weitergegeben.
Die von Nutzern eingeholte Einwilligung ist rechtswidrig gewesen, da sie eine Freiwilligkeitskomponente beinhalten muss.

Grindr machte jedoch die App-Nutzung von der Zustimmung in die Weitergabe personenbezogener Daten an Dritte abhängig, was nicht als Einwilligung gesehen werden kann.

ANMELDUNG GILT NICHT ALS ÖFFENTLICHE BEKANNTMACHUNG

Ein anderer Aspekt war die sexuelle Orientierung der Nutzer. Solche persönlichen Daten fallen in die Kategorie sensibler Daten gem Art 9 Abs 1 DSGVO. Die Verarbeitung solcher Daten ist grundsätzlich untersagt. Der Abs 2 sieht Ausnahmen vor, die die Verarbeitung von sensiblen Daten erlauben, unter anderem Einwilligung und offensichtliche öffentliche Bekanntmachung. Wie festgestellt, war die eingeholte Einwilligung mangels Freiwilligkeit rechtswidrig. Grindr begründete die Weitergabe sensibler Daten mit Art 9 Abs 2 lit e, da die Nutzer die Daten öffentlich bekanntgegeben haben. Auch dieses Argument konnte vor der norwegischen Datenschutzbehörde nicht standhalten, weil Grindr ein geschlossener Netzwerk ist, der den Nutzern Privatsphäre durch geschlossene Community garantiert. Deswegen kann das Anlegen von einem Account bei Grindr nicht als offensichtliche öffentliche Bekanntmachung gesehen werden.

Für das Unternehmen sind 10 Millionen Euro eine spürbare Strafe, da der Jahresumsatz laut Medien bei 31 Millionen US Dollar liegt. Die Entscheidung ist noch nicht rechtskräftig.

CLEARVIEW - NUTZUNG VON BIOMETRISCHEN DATEN

Der Hamburgische Beauftragte für Datenschutz und Information (HmbBfDI) hat ein Verfahren gegen die Clearview AI Inc. eingeleitet. Das Ziel ist die Löschung des mathematisch generierten Hash-Werts des Beschwerdeführers, sowie Bestätigung der Löschung gegenüber der HmbBfDI.

EINWILLIGUNG WURDE ZU KEINEM ZEITPUNKT ERTEILT

Als Anlass diente die Beschwerde des Matthias M aus Hamburg, der von seinem Recht auf Auskunft gem Art 15 DSGVO bei Clearview AI Gebrauch machte. Daraufhin bekam er die Auskunft mit positiven Einträgen zu seiner Person. Es handelte sich um mehrere Fotos aus unterschiedlichen Lebensabschnitten. Laut Matthias M hätte man diese auch durch die Google-Suche finden können, jedoch wurde die Einwilligung zur Verarbeitung durch Clearview AI zur keinem Zeitpunkt erteilt.

IDENTIFIZIEREN DURCH DEN HASH-WERT

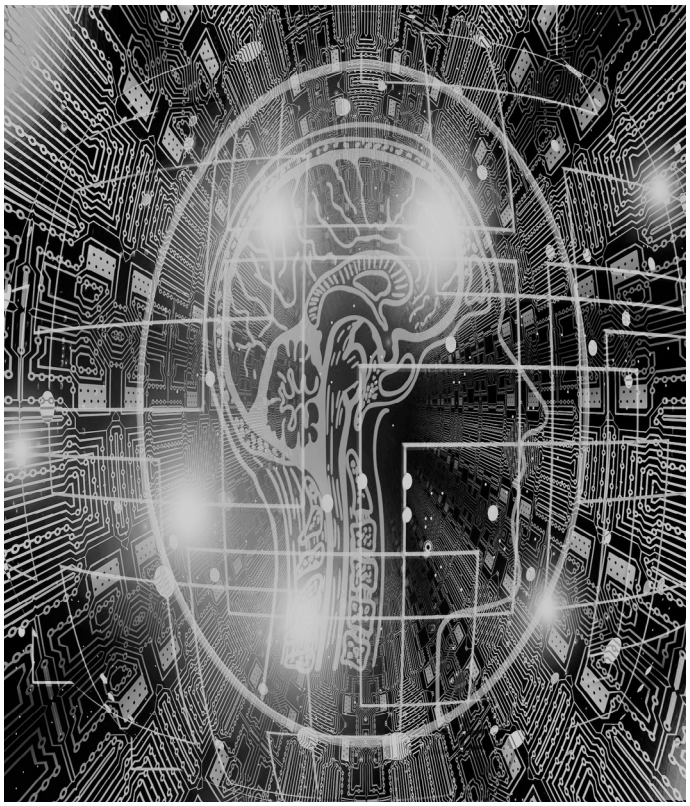
Bei Clearview AI handelt es sich um ein Start-up Unternehmen aus den USA, das große Mengen an Bildern verarbeitet, die für die Gesichtserkennung genutzt werden. Die Bilder werden ohne Einwilligung der Nutzer aus allen möglichen sozialen Netzwerken, Foren, Blocks und Unternehmensseiten in der Datenbank von Cleaview AI abgespeichert und mit entsprechenden Fund-Quelle versteht. Aus den gesammelten Daten wird ein einzigartiger Hash-Wert durch spezielle mathematische Verfahren entwickelt, der eindeutiges Identifizieren von Personen ermöglicht. Das Ganze funktioniert wie eine Suchmaschine, es wird ein Foto hochgeladen und mit etwas Glück bekommt man einen Treffer. Laut Medienangaben verfügt Cleaview AI zurzeit über 3 Millionen Bilder.

Dieser App wird bereits von mehreren Ländern für Aufspüren von Straftätern genutzt. Die Nutzung durch die Allgemeinheit ist bis jetzt nicht vorgesehen.

BEI DSGVO-ANWENDUNG KOMMT ES AUF VERARBEITUNG DER DATEN AN

Bei den Gesichtsbildern handelt es sich um biometrische Daten, da die dazu geeignet sind natürliche Personen eindeutig zu identifizieren. Solche Daten dürfen generell nur aufgrund der spezifischen Rechtsgrundlage gem Art. 9 Abs 2 DSGVO verarbeitet werden.

Im Vorfeld war zu klären, ob die DSGVO auf diesen Fall anwendbar ist, da Clearview Al. keine Niederlassung in der EU hat. Die DSGVO wird immer dann auf die „Verarbeitung personenbezogener Daten von betroffenen Personen angewendet, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt“ so die Datenschutzbehörde.



VERARBEITUNG BIOMETRISCHER DATEN IST UNZULÄSSIG

Die HmbBfDI hielt die Verarbeitung biometrischer Daten für unzulässig, sowie die Erstellung eines Hash-Werts und setzte eine Frist bis 12.2.2021 um die Löschung vorzunehmen.In einem Interview erzählt mit Matthias M., dass Clearview Al. dem Löschbegehren nachgekommen ist.

NUR MATHEMATISCH GENERIERTER HASH-WERT SOLL GELÖSCHT WERDEN

Man kann diese Entscheidung als einen Schritt in die richtige Richtung ansehen. Jedoch ist es nicht ganz nachvollziehbar, warum lediglich die mathematisch generierte Hash-Werte zur Person gelöscht werden sollen und nicht die vollständige Löschung der Fotos verlangt wurde, da die HmbBfDI die Gesichtsbilder als biometrische Daten ansah und die Verarbeitung nur unter strengen Voraussetzungen möglich ist.

Zudem ist die Entscheidung allgemein nicht anwendbar. Jeder einzelne, der seine Daten bei Clearview löschen lassen will, muss sich an die Datenschutzbehörde wenden.

INTERESSENSKONFLIKT MEINUNGSFREIHEIT UND RECHT AUF GEHEIMHALTUNG

In der Entscheidung (DSB-D124.2228) vom 21.4.2020 hatte die Datenschutzbehörde zu entscheiden, inwieweit das Medienprivileg das Recht auf Geheimhaltung einschränkt.

ONLINEZEITUNG VERÖFFENTLICHT AUDIOAUFNAHME DES GESPRÄCHS

Der Beschwerdegrund war ein Artikel der Online-Tageszeitung, der das Gespräch zwischen dem Beschwerdeführer und Polizeimitarbeitern wiedergab. Bei dem Beschwerdeführer handelte es sich um einen, zum Zeitpunkt der Beschwerde bereits ehemaligen, Polizeichef, der mit dem Polizeinotruf eine Polizeistreife anforderte. Da der Polizeimitarbeiter diesen nicht direkt an seiner Stimme erkennt und Zweifel an der Identität des Anrufers hat, drohte der Beschwerdeführer dem Polizeimitarbeiten Disziplinarverfahren an und bestellt ihn am nächsten Tag in sein Büro um Leviten zu lesen. Dem Online-Artikel wurde eine Aufnahme des Gesprächsmitschnitts angehängt.

DIE LÖSCHUNG WIRD VERWEIGERT

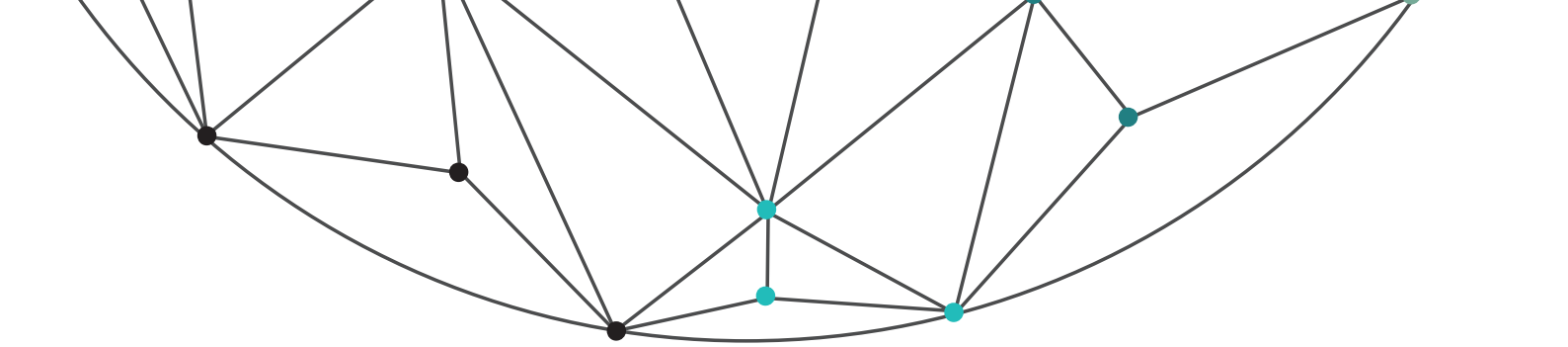
Der Beschwerdeführer forderte die Online-Zeitung per E-Mail auf den Artikel aufgrund des Art 17 DSGVO (Recht auf Vergessenwerden) zu löschen. Der Medieninhaber kam dem mit der Begründung der freien Meinungsäußerung nicht nach.

In diesem Fall musste das Interesse an der Geheimhaltung und offensichtlichen Verspottung der Meinungsfreiheit gegenüber gestellt werden.

INFORMATIONSFREIHEITSPRIVILEG NUR MEDIENUNTERNEHMEN VORBEHALTEN

Der § 9 DSG räumt ein Medienprivileg ein und knüpft an Art 85 DSGVO an. Demnach ist jede Verarbeitung personenbezogener Daten, die zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, zulässig. Man spricht von einem Informationsfreiheitsprivileg, welches im nationalem Recht nur auf Medienunternehmen und Mediendienste beschränkt ist.

Nach EuGH liegt eine Verarbeitung zur journalistischen Zwecken dann vor, wenn die ausschließlich das Ziel hat Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten (EuGH, 16. Dezember 2008, C-73/07).



WEITE AUSLEGUNG BEIM BEGRIFF MEINUNGS-ÄUSSERUNG

Das Recht auf freie Meinungsäußerung sowie der Begriff Journalismus muss weit ausgelegt werden, damit der Bedeutung dieses Rechts Rechnung getragen werden kann (EwGr 153 DSGVO). Die Verarbeitung zu journalistischen Zwecken liegt demnach immer vor, wenn die Veröffentlichung für einen unbestimmten Personenkreis bestimmt ist.

Bei dem Beschwerdegegner handelt es sich unverkennbar um ein Medienunternehmen. Die Daten wurden im Zusammenhang mit dem Artikel verarbeitet. Die Verspottung schadet dem nicht, da die Öffentlichkeit damit über die Missstände in der Verwaltung aufgeklärt wurde. Die Datenverarbeitung erfolgte zur journalistischen Zwecken und war deswegen zulässig.

DIE SPEICHERDAUER VON STAMMDATEN DURCH MOBILFUNKANBIETER

Im Bescheid (DSB-D124.024/0008-DSB/2019) hatte die Datenschutzbehörde über die zulässige Speicherdauer von personenbezogenen Daten beim Mobilfunkanbieter zu entscheiden.

LÖSCHUNG ERFOLGTE NUR TEILWEISE

Nach der Vertragsauflösung und Begleichung der letzten Rechnung beim Mobilfunkanbieter ersuchte der Beschwerdeführer um die Auskunft nach Art 15 DSGVO, die ihm fristgerecht erteilt wurde. In Folge begehrte der Beschwerdeführer die Löschung aller sich in der Auskunft befindlichen Daten. Der Beschwerdegegner kam der Löschung nur teilweise nach und begründete sein Vorgehen mit diversen rechtlichen Vorschriften, die zur längeren Aufbewahrung verpflichten. Gelöscht wurden lediglich die Verkehrsdaten, die Stammdaten blieben unberührt. Zudem gab der Beschwerdegegner keine Auskunft welche Art von Daten unter Verkehrs- und Stammdaten fallen.

Die Datenschutzbehörde hatte zu entscheiden ob in diesem Fall die Verletzung des Rechts auf Löschung vorliegt.

ERLÄUTERUNG VERKEHRS- UND STAMMDATEN

In erste Linie musste geklärt werden welche Arten von Daten durch den Mobilfunkanbieter verarbeitet werden und wie lange diese gespeichert werden dürfen. Bei den Verkehrsdaten handelt es sich nach § 92 Abs 3 Z 4 TKG um Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden. Es sind solche Daten wie E-Mail-Adressen, Datum und Uhrzeit des Zugriffs, Standortdaten usw.
Die Stammdaten sind personenbezogene Daten, die für den Abschluss, Durchführung, Änderung oder Beendigung des Vertrages erhoben wurden. Diese sind Name, akademischer Grad bei natürlichen Personen. Anschrift, Teilnehmernummer und sonstige Kontaktinformationen für die Nachricht, Information über die Art und Inhalt der Vertragsverhältnisse, Bonität, Geburtsdatum.

SPEICHERDAUER HÄNGT VON DATENART AB

Die Verarbeitung dieser personenbezogenen Daten ist streng an die Zwecke gebunden. Die Verkehrsdaten sind zu löschen oder zu anonymisieren, sobald das noch ausstehende Entgelt bezahlt wurde oder dieses innerhalb einer dreimonatigen Frist nicht schriftlich verlangt wurde. Dem Gesetzeswortlaut ist eine Frist von drei Monaten für die Löschung von Stammdaten zu entnehmen. Eine längere Speicherdauer widerspricht dem Art. 5 Abs 1 lit e DSGVO. Diese Daten wurden zum Zeitpunkt der Beschwerde bereits gelöscht und stellten keinen Entscheidungsgegenstand mehr dar.

Die Stammdaten können auf der Grundlage des § 132 Abs 1 BAO für die Dauer von sieben Jahren aufbewahrt werden. Nach Ablauf dieser Frist sind sie zu löschen. Für Speicherung von darüber hinausgehenden Daten, die keine Stamm- oder Verkehrsdaten sind, fehlt jedoch die rechtliche Grundlage. Die Aufbewahrung dieser Daten würde dem Prinzip der Speicherbegrenzung nach Art 5 Abs 1 lit e DSGVO widersprechen (DSB-D216.471/0001-DSB/2018).

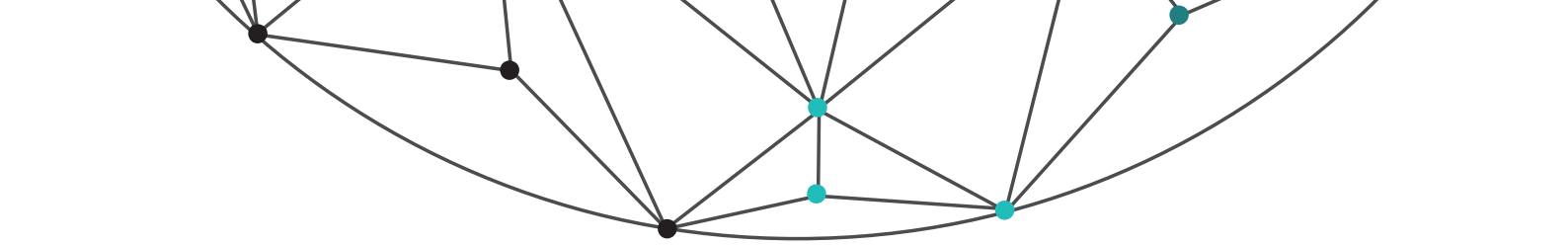
EINSICHT IN PATIENTENAKTE FÜR NEGATIVE GOOGLEBEWERTUNG UNZULÄSSIG

Im Bescheid (DSB 2020-0.251.582) entschied die Datenschutzbehörde über die Zulässigkeit der Einsicht in die Patientenakte, wenn diese Einsicht nicht den Behandlungszwecken dient.

Die Beschwerdeführerin befand sich in Behandlung bei der Beschwerdegegnerin, eine Ärztin mit eigener Ordination. Die Beschwerdeführerin konnte den Termin nicht wahrnehmen und kontaktierte die Ordination um einen neuen Termin zu vereinbaren. Beim Telefonat mit dem Ordinationsmitarbeiter kam es zum Disput, da dieser keinen neuen Termin aufgrund des versäumten Termins vom Vortag vergeben wollte. Aus diesem Anlass gab die Beschwerdeführerin eine negative Bewertung über die Ordination bei Google ab.

Daraufhin entnahm der Ordinationsmitarbeiter aus der Patientenakte die Daten des Arbeitgebers der Beschwerdeführerin und gab auf Google eine negative Bewertung „Mitarbeiterin N.A. hält Termine nicht ein – nicht weiter zu empfehlen“ ab.

Die Datenschutzbehörde hatte zu entscheiden, ob dadurch das Recht auf Geheimhaltung verletzt wurde.



EINSICHT WIRD DER ÄRZTIN ZUGERECHNET

Das Vorgehen des Ordinationsmitarbeiters wurde der Ärztin (Beschwerdegegnerin) zugerechnet, weil die Verarbeitung von personenbezogenen Daten weder dem eigenen Zweck des Mitarbeiters diente, noch außerhalb der Tätigkeit der Ärztin verarbeitet wurde.

DURCH DIE BEWERTUNG IST DAS RECHT AUF GEHEIMHALTUNG VERLETZT

Der Ordinationsmitarbeiter hat die personenbezogenen Daten mit dem Zweck verarbeitet, um eine negativen Bewertung als Retorukutsche auf die negative Bewertung der Beschwerdeführerin abzugeben.

Das Recht auf Datenschutz gem § 1 Abs 1 DSG gewährt jedermann ein Anspruch auf Geheimhaltung der ihn betreffenden Daten, um Achtung seines Privat- und Familienlebens zu bewahren. Dabei handelt es sich jedoch um kein absolutes Recht, es kann durch zulässige Eingriffe beschränkt werden. Eine zulässige Beschränkung liegt vor, wenn die nicht im lebenswichtigen Interesse des Betroffenen liegt oder mit seiner Zustimmung erfolgt und zur Wahrung überwiegender berechtigter Interessen eines anderen erfolgt (§ 1 Abs 2 DSG). Einsicht in die Patientenakte zwecks negativer Bewertung stellt unter keinen Umständen ein zulässiger Eingriffstatbestand dar. Somit lag eine Verletzung des Rechts auf Geheimhaltung vor. Während des Verfahrens wurde die negative Bewertung über die Beschwerdeführerin zwar entfernt, nach der Ansicht der Datenschutzbehörde ändert jedoch die Löschung nichts an der Rechtsverletzung und wird dadurch nicht ungeschehen gemacht.

AMS-ALGORITHMUS OHNE GEEIGNETE RECHTSGRUNDLAGE

Im Bescheid (DSB-D213.1020) vom 16 August 2020 hatte die Datenschutzbehörde über die Zulässigkeit des Arbeitsmarktchancen Assistenz-Systems („AMAS“) entschieden.

WAHRSCHEINLICHKEIT BESTIMMT DIE BESCHÄFTIGUNGSDAUER

Der Algorithmus soll die Einschätzung der Arbeitsmarktchancen von Arbeitssuchenden unterstützen und dadurch die AMS-Ressourcen besser und effizienter nutzen. Das System sollte mit personenbezogenen Daten wie Altersgruppe, Geschlecht, Staatengruppe, Ausbildung, Gesundheitliche Beeinträchtigung, Betreuungspflichten, Berufsgruppe, Vorkarriere, regionales Arbeitsmarktgeschehen und die Dauer des Geschäftsfalles bei AMS „gefüttert“ werden. Anhand dieser Daten wird die Wahrscheinlichkeit (niedrig, mittel, hoch) ausgerechnet welche Anzahl an Tagen die beim AMS vorgemerkten Kunden in Zukunft beschäftigt sein können. Diese Ergebnisse können von Beratern für Bearbeitung der Fälle herangezogen werden.

VERARBEITUNG NUR DURCH KLARE GESETZLICHE ERMÄCHTIGUNG MÖGLICH

AMS ist eine Behörde, aus diesem Grund reicht eine bloße gesetzliche Ermächtigung für Datenverarbeitung nicht aus. Vielmehr muss es hinreichend determiniert sein unter welchen Voraussetzungen die Verarbeitung personenbezogener Daten vorgenommen werden darf. Die entsprechende Rechtsgrundlage oder Gesetzesmaßnahme sollte klar und präzise sein sowie durch die Rechtsprechung Europäischer Gerichte für den Rechtsunterworfenen vorhersehbar sein (Erwägungsgrund 41 DSGVO).

Die von AMS als gesetzliche Grundlage angeführte Paragraphen (§§ 25 Abs 1, 29 und 31 Abs 5 AMSG) eignen sich für die zwangsläufige Verarbeitung von Daten, die für gestellte Leistungsanträge notwendig sind. Jedoch reichen die angeführten Rechtsvorschriften für die Errechnung von Arbeitsmarktchancen nicht aus, weil es sich nicht um bloße Verarbeitung der Daten, sondern Profiling handelt.

SCHWERER EINGRIFF MUSS VORHERSEHBAR SEIN

Profiling ist eine automatisierte Verarbeitung personenbezogener Daten um bestimmte persönliche Aspekte wie Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit usw zu ermitteln und stellt einen großen Eingriff in das Grundrecht auf Datenschutz dar. Dadurch muss der Eingriff für den Betroffenen deutlich vorhersehbar und die Rechtsgrundlage strengeren Anforderungen unterzogen sein.

NATIONALER GESETZGEBER MUSS ABSTUFUNGEN IN DER DSGVO EINHALTEN

Die DSGVO zieht eine klare Differenzierung zwischen „bloßer“ Verarbeitung von Daten und Profiling. Wenn der europäische Verordnungsgeber einen solchen Unterschied macht, muss das Gleiche auch vom nationalen Gesetzgeber eingehalten werden. Die von AMS angeführte Rechtsgrundlage enthält nur die Ermächtigung zur Verarbeitung der Daten, was nach dem angeführten Argument für Profiling nicht ausreicht.

ANWENDUNG FÜR WICHTIGEN LEBENSBEREICH SEHR FRAGWÜRDIG

Abgesehen von der fehlenden gesetzlichen Grundlage ist die Anwendung solcher Systeme mehr als fraglich. Bei der Zusendung von Werbung wäre es weniger tragisch, da man die Produkte nicht erwerben braucht. Bei der Arbeitssuche geht es um die Existenz der Menschen, die den Lebensverlauf und die Lebensqualität stark beeinflussen.

Dadurch dürfen solche Entscheidungen nicht einer Maschine überlassen werden. Zwar werden dazu noch persönliche Gespräche geführt, jedoch kann man nicht sagen inwiefern die Berater sich von der Wahrscheinlichkeitsrechnung beeinflussen lassen und nicht mehr genau nachfragen, vielleicht auch um der Algorithmus-Rechnung nicht zu widersprechen. Es hat den Charakter eines Schubladensystems: Daten eingeben, Maschine rechnet aus und Lade zu.

AUS FÜR DIE PNR-RICHTLINIE?

Bereits 2016 verabschiedete der Europäische Gesetzgeber eine Richtlinie zur Speicherung von Fluggästedaten (Passenger Name Record, PNR) bei Flügen in und aus der EU. Anfang des Jahres 2020 ersuchte das Amtsgericht Köln um Vorabentscheidung durch EuGH ob die PNR-Richtlinie mit Grundrechten der Europäischen Union vereinbar werden kann. Der Zweck der Richtlinie ist die Vorbeugung, Verhinderung und Aufklärung von terroristischen und bestimmten anderen Straftaten.

GEGENSTAND DES RECHTSSTREITS VOR AMTSGERICHT KÖLN

Der Betroffene buchte einen Flug von München nach Ankara und retour und ersuchte das Flugunternehmen seine Daten nicht an das deutsche Bundeskanzleramt zu übermitteln, das Flugunternehmen kam dem Ersuchen nicht nach.

Das Amtsgericht Köln stellte insgesamt fünf Fragen an den EuGH, unter anderem ob der Umfang gespeicherter Daten verhältnismäßig zum angestrebten Zweck ist, ob die Richtlinie einen ausreichenden Rechtsschutz vorsieht und inwiefern das Schutzniveau der europäischen Grundrechte durch die Datenspeicherung gewährleistet ist.

UMSETZUNG DER RICHTLINIE IN ÖSTERREICH

Im österreichischen Recht wurde die Richtlinie im PNR-Gesetz umgesetzt.

Die Flugunternehmen sind verpflichtet Passagierdaten an die nationale Behörde zu übermitteln. Die Flugdatenzentralstelle ist bei Bundesministerium für Inneres eingerichtet, für Organisatorisches ist das Bundeskanzleramt zuständig.

Die Liste der zu übermittelnden Daten ist lang, angefangen mit Namen und Adresse reicht die Übermittlung bis zu Angaben zum Reisebüro, Gepäckangaben und Daten von Mitreisenden. Um im „Flugdatenregister" aufzuscheinen, muss die Person eine Reise aus der EU in Mitgliedstaat oder zurück vorgenommen haben. In Österreich hat der Bundesministerium für Inneres die Anwendung des PNR-Gesetzes auf die Flüge innerhalb der Union ausgeweitet.

DATEN MÜSSEN FÜNF JAHRE AUFBEWAHRT WERDEN

Die Daten werden prophylaktisch gespeichert, es müssen keine Hinweise auf mögliche Verbindungen zu terroristischen Gruppierungen vorliegen. Die Speicherung erfolgt somit auf Vorrat, nach einem halben Jahr müssen die Daten depersonalisiert werden. Sie werden nicht komplett aus dem System gelöscht, sondern nur unkenntlich gemacht, so dass die Identität der betroffenen Person nicht festgestellt werden kann, eine Rückgängigmachung jedoch möglich ist. Die Daten müssen insgesamt fünf Jahre gespeichert sein, eine ausdrücklich Löschungspflicht sieht die Richtlinie nicht vor. Das PNR-Gesetz verweist auf § 50 DSG und regelt eine explizite Löschung nach fünf Jahren.

DIE ZUKUNFT DER RICHTLINIE UNGEWISS

Der EuGH hatte bereits 2017 ein Abkommen über den Austausch von Flugdaten zwischen Union und Kanada wegen dem Eingriff in die EU-Grundrechte gekippt. Ob der EuGH auch die PNR-Richtlinie für unzulässig erklärt lässt sich schwer vorher sagen. Aus datenschutzrechtlicher Sicht wäre es ein Erfolg um der staatlichen Überwachung beim Reisen zu entkommen.

ÖSTERREICHISCHE POST AG ENTSCHEIDUNG DES BVWG

Der Aufreger des Jahres 2019, von dem die ARGE DATEN im Tätigkeitsbericht 2019/2020 berichtete, war die Berechnung der Parteienaffinität durch die Österreichische Post AG. Dabei wurden Daten im großen Stil verarbeitet und an die Unternehmen sowie politische Parteien verkauft.

Die Datenschutzbehörde schob dem einen Riegel vor und sprach eine Strafe in Hohe von 18 Millionen Euro aus. Die Österreichische Post AG erhob dagegen eine Beschwerde beim Bundesverwaltungsgericht.

KEINE STRAFE OHNE NENNUNG NATÜRLICHER PERSON ALS HANDELNDE ORGANE

In seiner Entscheidung (W258 2227269-1/14E) vom 26.11. 2020 hob das BVwG die verhängte Strafe auf und stellte das Verfahren ein. Begründet wurde die Entscheidung damit, dass für die Verhängung einer Geldbuße alle notwenigen Elemente einer Bestrafung (tatbestandsmäßig, rechtswidrig, schuldhaft) im Spruch erhalten sein müssen mit dem Zusatz, dass das Verhalten natürlicher Person der juristischen Person zugerechnet wird. Dabei verwies das BVwG auf ein früheres Urteil des VwGH vom 29.03.2019 (Ro 2018/02/0023).

Die Datenschutzbehörde hat es unterlassen in ihrem Straferkenntnis eine natürliche Person zu benennen, erst im Beschwerdeverfahren wurde der Mangel nachgeholt, was eine unzulässige Änderung des Tatvorwurfs darstellte.

KEIN VORABENTSCHEIDUNGSVERFAHREN TROTZ UNKLARER GESETZESAUSLEGUNG

Dieses Urteil wirft einige Fragen auf. Zum ersten warum BVwG die Frage nicht zum Vorabentscheidungsverfahren dem EuGH vorgelegt hat. In dieser Rechtssache gibt es bis jetzt keine einheitliche Rechtsprechung. Die aus Sicht des BVwG auch nicht notwendig ist, da gemäß Art 83 Abs 8 DSGVO bei Verhängung von Geldbußen die innerstaatlichen Vorschriften eingehalten werden müssen.

Das ist nicht ganz nachvollziehbar, weil Abs 8 lediglich von angemessenen Verfahrensgarantien, wirksamer Rechtsbehelfe und einem ordnungsmäßigen Verfahren spricht. Es soll also gewährleistet werden, dass das Verfahren den rechtsstaatlichen Grundsätzen entsprechend abgehalten wird. Die DSGVO selber spricht bei der Haftung nur vom Verantwortlichen und nimmt keine Unterscheidung zwischen natürlichen und juristischen Personen vor. Die Auslegung aus Sicht des BvWG ufert insofern aus, dass aus der Bestimmung abgeleitet wird unter welchen Voraussetzungen Geldbußen überhaupt verhängt werden dürfen. Damit öffnet man dem nationalen Gesetzgeber Tür und Tor die DSGVO auszuhöhlen und die Bestrafung von Verantwortlichen, anders als vom europäischen Gesetzgeber geplant, nach eigenen Vorlieben zu regeln.

VON AUSSERORDENTLICHER REVISION WURDE KEIN GEBRAUCH GEMACHT

Die zweite Frage ist warum die Datenschutzbehörde kein Rechtsmittel gegen die Entscheidung erhoben hat. Die ordentliche Revision wurde durch das BVwG zwar ausgeschlossen, jedoch bestand die Möglichkeit einer außerordentlichen Revision. Aus Sicht der DSB wäre das nicht besonders zielführend, da VwGH in einer ähnlichen Sache (D550.038/0003-DSB/2018) bereits entschieden hat und nunmehr auf die Vorentscheidung verwiesen hätte.

STRAFEN WURDEN BEREITS AUS GLEICHEM GRUND AUFGEHOBEN

Und die letzte abschließende Frage wäre, warum die Datenschutzbehörde bei so einem bedeutenden Fall nicht aus den Fehlern der Vergangenheit lernt. In der ähnlichen Entscheidung (D550.038/0003-DSB/2018) wurde nur gegen eine juristische Person, ohne Angaben der natürlichen Person, Geldbuße verhängt. Das BVwG hob die Geldstrafe auf und stellte das Verfahren ein. Die Datenschutzbehörde erhob zwar eine Revision bei VwGH, dieser bestätigte jedoch die Entscheidung des BVwG und wies die Revision mit der Begründung ab.

Bei DSGVO geht es nicht um Geldbußen an sich, sonders eindeutig um Strafen, deswegen muss einer juristischen die natürliche Person zugerechnet werden. Der DSB war also bereits 2018 bekannt, dass die Straferkenntnisse ohne Erforschung und Angaben natürlicher Personen vor BVwG nicht standhalten werden und unterließ es auch dieses mal. Da war der Fall von Anfang an zum Scheitern verurteilt. Es bleibt nur zu hoffen, dass doppelt besser hält und die nächste Geldbuße vorschriftsmäßig verhängt wird.

DATENSKANDAL: ERGÄNZUNGSREGISTER ÖFFENTLICH ZUGÄNGLICH

Die epicenter.works - Plattform Grundrechtspolitik berichtete von einem jahrelang unentdeckt gebliebenen Datenschutzskandal. Die Daten des „Ergänzungsregisters für sonstige Betroffene" konnten im Netz frei eingesehen werden. Dabei handelt es sich um ein Sammelregister für juristische Personen, die sich in kein anderes Sammelregister (Firmenbuch, ZVR) eintragen können, jedoch eine digitale Identität brauchen.

Weiters befinden sich auch natürliche Personen im Register, die Einkünfte aus Land- und Forstwirtschaft, selbständiger Tätigkeit, aus Gewerbebetrieb oder Vermietung und Verpachtung hatten und sonst nirgends eingetragen sind.

AUCH PRIVATE ADRESSEN WAREN ÖFFENTLICH

Die Datensätze waren ohne jeglichen Schutz über Jahre öffentlich zugänglich. Jeder konnte die privaten Adressen abrufen oder anhand der Daten ableiten, wann die Steuererklärung gemacht oder Beihilfe bezogen wurde. Schätzungsweise geht es um über eine Million Betroffene, die genauen Zahlen lagen zum Zeitpunkt der Berichterstattung nicht vor.

AUCH NACH BEENDIGUNG UNTERNEHMERISCHER TÄTIGKEIT KEINE LÖSCHUNG

Die Eintragung wurde hauptsächlich durch öffentliche Stellen vorgenommen. Auf die Löschung der Daten wurde kein besonderes Augenmerk gelegt, so waren Personen im Register zu finden, deren unternehmerische Tätigkeit schon lange aufgegeben wurde. Es ist auch der Tatsache geschuldet, dass nicht genau definiert ist wann die unternehmerische Tätigkeit nicht mehr vorliegt, es könnten theoretisch noch Insolvenzverfahren geführt werden oder Ansprüche von MitarbeiterInnen bestehen.

SYSTEM WURDE AB 2013 VERSTÄRKT MIT DATENSÄTZEN GESPEIST

Das Ergänzungsregister wurde 2004 eingeführt, die Führung erfolgte ausschließlich online. Zu dem Zeitpunkt befanden sich nur wenige Einträge in Register. Erst ab 2013 nahm die Speicherung rasant zu und verzeichnete circa 1,4 Millionen Datensätze. Diese Zunahme an Einträgen ist auf die automatische Speicherung durch das Finanzministerium zurückzuführen.

KEIN NACHVOLLZIEHBARER GRUND FÜR ÖFFENTLICHE FÜHRUNG

Es kann nicht nachvollzogen werden aus welchem Grund das Ergänzungsregister überhaupt öffentlich geführt wurde. Als Argument wurden Konsumentenschutz und öffentliche Evidenz vorgebracht, jedoch ohne Begründung.

Wegen des steigenden öffentlichen Interesses ist das Abrufen des Registers vorerst nicht mehr möglich. An der Lösung des Problems und Lösungen zur weiteren Nutzung wird gearbeitet.

DEUTSCHLAND: SICHERHEITSLÜCKEN BEI HOCHSCHULEN UND ROTEM KREUZ

Der Deutsche Verein für Datenschutz e.V berichtete in seinem Magazin (DANA 2/2020) von zwei großen Datenschutzpannen, die im Jahr 2020 bekannt wurden.

STUDENTENDATEN WAREN 9 JAHRE LANG FREI ABRUFBAR

Die erste Datenschutzlücke betraf die deutschen Hochschulen, die das Hochschul-Informations-System (HIS) nutzten, sie soll aufgrund eines Konfigurationsfehlers entstanden sein. Dadurch konnten Unbefugte auf die Daten von mehr als 600.000 Studierenden über 9 Jahre lang zugreifen.

Es handelte sich um solche Daten wie Namen, Adressen, Geburtsdaten, Matrikelnummer und Immatrikulationsstatuts, die ins Jahr 1991 reichten. Finden konnte man all diese Daten durch die Eingabe des richtigen Links.

Die Sicherheitslücke bestand seit neun Jahren. Es lässt sich nicht sagen inwiefern die Daten für rechtswidrige Zwecke gebracht wurden. Mit diesen Daten wäre zum Beispiel der Identitätsdiebstahl, das Abfragen der Noten und der Studiendauer möglich.

Nach DSGVO müssen Verantwortliche den Vorfall innerhalb von 72 Stunden der zuständigen Datenschutzbehörde melden. Nach Eigeneingaben der Hochschulen wurden die Fristen eingehalten. Als Begründung für die Speicherung von 30 Jahre alten Daten gaben Hochschulen die Nachweisnotwendigkeit von Studien- und Versicherungszeiten an.

Die Hochschulen unterließen es die Studierenden über die Offenlegung der Daten zu informieren. Nach dem Gesetz sind keine Strafen gegen die staatlichen Hochschulen vorgesehen. Die Möglichkeit den Schadenersatz geltend zu machen bleibt bestehen, jedoch muss der Nachweis des tatsächlichen Schadens erbracht werden.

Die Sicherheitslücken wurden von den Hochschulen umgehend geschlossen.

DAS DEUTSCHE ROTE KREUZ NAHM DIE IT-SICHERHEIT AUF DIE LEICHTE SCHULTER

Ähnliches Problem stellte sich beim Deutschen Roten Kreuz (DRK). Durch zu schlechte IT-Sicherheit war es den Hackern möglich auf personenbezogene Daten von mehr als 30.000 Betroffenen zuzugreifen.

Ein 18-jähriger Hacker machte die DRK-Kreisverbände auf die Sicherheitslücke aufmerksam, als Reaktion wurde lediglich der Zugang zu einer Seite gesperrt. Auch nach dem kurzen Video vom Hacker, wie dieser innerhalb von 3 Minuten die Datenbank hackt, blieb das Problem bestehen. Deswegen suchte er den Kontakt zu Journalisten um von der Sicherheitslücke zu berichten.

Man konnte problemlos auf Namen, Adressen, Geburtsdaten, Angaben zur Krankenkasse des Patienten oder ob der Patient im Rollstuhl sitzt oder an einer Viruserkrankung leidet, zugreifen. Über den Zugriff auf den Server wäre es dem Hacker sogar möglich gewesen die Angaben in Echtzeit zu verändern, wie zum Beispiel die Krankentransporte abzubestellen oder zu manipulieren.

Auch in diesem Fall lässt sich nicht mehr verfolgen, ob Kriminelle die Daten missbraucht haben. Die Journalisten fanden jedoch heraus, dass die Zugangsdaten des DRK-Administrators auf einer türkischsprachigen Webseite bereits 2017 veröffentlicht wurden.

Mittlerweile sollen laut DRK alle Sicherheitslücken geschlossen sein, auch die Meldung an die Datenschutzbehörde wurde getätigt, jedoch die Meldefrist von 72 Stunden überschritten.

Diese Vorfälle sind sehr alarmierend und zeigen nochmal, dass viele Unternehmen und Einrichtungen den Schutz der personenbezogenen Daten nicht so ernst nehmen, wie es gewünscht ist. Sogar bei offensichtlichen Lücken und mehrmaligen Anzeigen durch außenstehende Personen, scheint es die Verantwortlichen nicht zu interessieren oder es wird der Anschein gemacht, dass man an der Problembehebung arbeitet.

EUGH UND OLG URTEIL IN CAUSA FACEBOOK

2020 wurden zwei bedeutende Entscheidungen im Rechtsstreit zwischen Max Schrems und Facebook bzw den Datenschutzbeauftragten von Irland gefällt. Max Schrems bezweifelte das angemessene Datenschutz-Schutzniveau von Vereinigten Staaten und ersuchte Commissioner von Irland Weitergabe seiner Daten durch Facebook Irland an Facebook Inc. in Vereinigten Staaten zu unterbinden. Der Commissioner wendete sich an EuGH.

Beim OLG brachte Max Schrems vor, keine Einwilligung in die Datenverarbeitung erteilt zu haben und verlangte Schadenersatz für die Unsicherheit bei Datenverarbeitung.

ANWENDBARKEIT VON DSGVO GEGEBEN

Der Europäische Gerichtshof hielt zunächst fest, dass die DSGVO auch dann anzuwenden ist, wenn an die Drittländer übermittelte Daten durch die Behörden dieses Drittstaates für die Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates verarbeitet werden.

BINDUNG DER NATIONALEN AUFSICHTSBEHÖRDEN AN ANGEMESSENHEITSBESCHLUSS

Die personenbezogenen Daten dürfen an die Drittländer dann übermittelt werden, wenn ein Angemessenheitsbeschluss vorliegt. Dieser kann von der Kommission nur erlassen werden, wenn die Rechtsvorschriften des einschlägigen Drittlandes alle für die Datenübermittlung erforderlichen Garantien bieten. Es wird verbindlich festgestellt, dass Drittland ein angemessenes Schutzniveau bietet. Solange dieser Beschluss nicht vom Gericht aufgehoben wurde, können Mitgliedstaaten keine Maßnahmen treffen, die darauf Bezug nehmen, dass der Drittstaat kein ausreichendes Schutzniveau hat und die Übermittlung der Daten infolgedessen zu untersagen sind. Jedoch kann die Kommission die betroffenen Personen nicht daran hindern Schutz ihrer Rechte und Freiheiten bei Verarbeitung der Daten geltend zu machen. Auch beim Vorliegen eines gültigen Angemessenheitsbeschlusses der Kommission muss die zuständige nationale Aufsichtsbehörde die mögliche Rechtsverletzung in völliger Unabhängigkeit prüfen und bei Unklarheiten um die Vorabentscheidung beim EuGH ansuchen.

KEINE DATENÜBERTRAGUNG OHNE NÖTIGE GARANTIEN

Liegt kein gültiger Angemessenheitsbeschluss der Kommission vor, ist die zuständige Behörde verpflichtet die Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn der erforderliche Schutz der übermittelten Daten im Sinne des Unionsrechts nicht gewährleistet werden kann.

STANDARDDATENSCHUTZKLAUSEL BINDET NUR DIE VERTRAGSPARTEIEN

Die Kommission kann auch Standarddatenschutzklauseln (SDK) erlassen, dabei ist die Kommission nicht verpflichtet das Schutzniveau des Drittlandes festzustellen. Die Klauseln sind für den Verantwortlichen und Empfänger verbindlich, wenn sie zum Vertragsinhalt werden. Für die Behörden des Drittlandes sind die SDK nicht verbindlich, da diese nicht Vertragspartei sind.

Der SDK-Beschluss zielt nur darauf ab den Parteien vertragliche Garantien, unabhängig vom Schutzniveau des Drittlandes, zu bieten. Aus diesem Grund kann es erforderlich sein dem Verantwortlichen zusätzlich Schutzmaßnahmen aufzutragen.

Kann der Verantwortliche oder Auftragsverarbeiter keine hinreichenden Schutzmaßnahmen ergreifen oder garantieren, muss die Datenübermittlung ausgesetzt oder beendet werden. Zudem muss der im Drittland Ansässige jede relevante nationale Rechtsänderung dem Verantwortlichen bekanntgeben. Diese Tatsachen berechtigen zum Rücktritt vom Vertrag.

DATENSCHUTZSCHILD BIETET KEINE RECHTSSCHUTZMÖGLICHKEITEN

Beim Datenschutzschild-Beschluss (DSS-Beschluss, „EU-US-privacy shield") der Europäischen Kommission handelt es sich um einen Angemessenheitsbeschluss. Dieser bindet die Aufsichtsbehörden insofern, als in dem Beschluss festgestellt wird, dass die Vereinigten Staaten ein ausreichendes Schutzniveau bieten. Das Regelungswerk des Schutzschilds besteht aus den Grundsätzen, die das amerikanische Handelsministerium für amerikanische Unternehmen als verbindliche Datenschutzregeln herausgegeben hat. Diese Grundsätze können jedoch bei Gefährdung nationaler Sicherheit, öffentlicher Interessen oder Durchführung von Gesetzen beschränkt werden. Diese Ausnahme ermöglicht es in die Grundrechte von Personen, deren Daten aus der EU übermittelt wurden, einzugreifen und diese zu verwenden.

Den Betroffenen werden keine Rechte verliehen, die gegenüber den amerikanischen Behörden durchgesetzt werden können. Es bestehen auch keine klaren Eingrenzungen in welchem Umfang die Erhebungen personenbezogener Daten vorgenommen werden. Der EuGH erachtet es als problematisch, weil es dem Wesen des Rechtsstaats widerspricht, wenn keine gerichtliche Kontrolle vorgesehen ist. Die Rechtsbehelfe im Drittland sind besonders wichtig, da die Verwaltungsbehörden oder Gerichte der Mitgliedstaaten bei rechtswidriger Datenverarbeitung keine Durchsetzungsmöglichkeiten im Drittland haben werden.

Aufgrund der mangelnden Rechtsschutzmöglichkeit erachtet der EuGH den Datenschutzschild zwischen EU und Vereinigten Staaten als ungültig.

OLG: VERTRAG ZWISCHEN NUTZER UND FACEBOOK IST WIRKSAM

Max Schrems machte in der Klage geltend, keine wirksame Einwilligung in die Verarbeitung seiner Daten erteilt zu haben. Facebook berief sich auf vertragliche Verhältnisse und rechtmäßige Datenverarbeitung gemäß Art 6 Abs 1 lit b DSGVO.

Das OLG bestätigte die Ansicht von Facebook und befand den zwischen den Nutzern und Facebook abgeschlossenen Vertrag als zulässig. Der Vertrag beruht darauf, dass die Nutzer die Facebook Dienste unentgeltlich nutzen können und im Gegenzug die Verwendung personenbezogener Daten für Werbezwecke dulden. Die Daten werden ohne ausdrückliche Zustimmung nicht an Dritte weitergegeben. Facebook senden in so einem Fall die Werbung im Auftrag des Werbekunden an die Nutzer weiter. Dieses Vertragsmodel ist weder ungewöhnlich noch sittenwidrig, deswegen gilt der Vertrag als wirksam abgeschlossen.

FACEBOOK MUSS SCHADENERSATZ ZAHLEN

Max Schrems wendete sich an das OLG und machte unter anderem geltend, dass die Unsicherheit bei Verarbeitung seiner Daten durch Facebook bei ihm einen emotionalen Unmut verursacht und verlangte deshalb einen Schadenersatz von 500 Euro.

Das OLG sah den immateriellen Schaden im Sinne von Art 82 Abs 1 DSGVO als gegeben, weil die Auskunft nicht vollständig erteilt und gab der Klage in diesem Punkt statt.

Max Schrems hat sich mittels ordentlicher Revision an den OGH gewendet. Er hofft, dass die Frage der rechtmäßigen Einwilligung im Zuge der Vorabentscheidung dem EuGH vorgelegt wird.

DEUTSCHLAND: EINSATZ VON WÄRMEBILDKAMERAS BZW. TEMPERATURMESSUNG WÄHREND CORONA

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat eine Bewertung über den Einsatz von Wärmebildkameras bzw Temperaturmessung für die Zutrittskontrollen in Flughäfen, Geschäften und Behörden abgegeben.

ANGABEN ZUR KÖRPERTEMPERATUR SIND PERSONENBEZOGENE DATEN

Zwar werden durch die Temperaturmessung keine eindeutig identifizierbaren Daten wie Name, Adresse usw verarbeitet, jedoch kann die Person über andere Quellen erkannt werden, etwa durch Personal, Kameraaufnahmen, Aufzeichnungen zur Messung oder Speicherung von Infrarot-Kameras. Deswegen stellt die Temperaturmessung eine Verarbeitung personenbezogener Daten nach Art 4 Z 1 und 2 DSGVO dar. Zudem müssen die Voraussetzungen für die Verarbeitung von Gesundheitsdaten erfüllt sein, weil die Messung der Körpertemperatur darauf gerichtet ist die potentiellen Infizierten auszusondern. Anderes würde gelten, wenn die Temperaturmessung ohne Protokollierung stattfinden würde, was in der Corona-Pandemie nicht zielführend wäre.

KEINE VERARBEITUNG AUFGRUND FREIWILLIGER EINWILLIGUNG

Die Verarbeitung personenbezogener Daten kann durch die Einwilligung gerechtfertigt werden. In den meisten Fällen wird die Einwilligung an der Freiwilligkeit scheitern. Problematisch ist die Einwilligung auch bei zahlreichen Beschäftigungsverhältnissen, kaum ein Arbeitnehmer würde die Zutrittskontrollen des Arbeitgebers, durch ein Ungleichgewicht geprägt, verweigern können. Die Temperaturmessung beim Zutritt zu einer Behörde kann nicht mit freiwilliger Einwilligung einhergehen, da die Betroffenen eine gesetzlich vorgesehene staatliche Leistung in Anspruch nehmen wollen oder einer Ladung folgen. Beim Zutritt in ein Geschäftslokal kann die Einwilligung ausdrücklich erteilt werden, kommt aber aus pragmatischen Gründen nicht in Frage.

Die Temperaturmessung bei Zugangskontrollen für die Erfüllung eines bestehenden Vertragsverhältnisses zwischen den Parteien (Art 6 Abs 1 DSGVO) scheidet aus. Diese rechtliche Grundlage könnte höchstens auf Beschäftigtenverhältnisse im nicht öffentlichen Sektor angewendet werden.

FÜR 6 ABS 1 LIT C MUSS NATIONALE REGELUNG VORLIEGEN

Viele Unternehmen beriefen sich auf die rechtliche Verpflichtung des Art 6 Abs 1 lit c DSGVO. Diese Vorschrift stellt jedoch keine rechtliche Verarbeitungsgrundlage dar, sondern setzte eine Rechtsgrundlage im bereichsspezifischen EU Recht oder im Recht eines Mitgliedstaates voraus (Art 6 Abs 3 DSGVO). Solche Regelungen sieht das deutsche Recht nicht vor.

VERARBEITUNG BEIM LEBENSWICHTIGEN UND ÖFFENTLICHEN INTERESSE

Die Datenverarbeitung zum Schutz lebenswichtiger Interessen der Betroffenen oder anderer natürlicher Personen nach Art 6 Abs 1 lit d DSGVO muss aufgrund der Verarbeitung von Gesundheitsdaten die Einwilligung der betroffenen Person vorliegen, außer diese ist nicht im Stande die Einwilligung zu erteilen. Auch diese Rechtsgrundlage kann nicht herangezogen werden.

Für die Verarbeitung im öffentlichen Interesse bedarf es, wie mit der rechtlichen Verpflichtung, einer klaren Regelung durch die EU oder Mitgliedstaaten, aus der ein Verarbeitungszweck abgeleitet werden kann. Bei Zutrittsregelungen zu Gebäuden der öffentlichen Verwaltung kann im deutschen Recht auf die datenschutzrechtliche Klausel zurückgegriffen werden. Es ist die Aufgabe jeder öffentlichen Stelle einen ordnungsmäßigen Dienstbetrieb zu organisieren. Unter der Beachtung des Grundsatzes der Erforderlichkeit bestehen jedoch erhebliche Zweifel an der elektronischen Messung der Körpertemperatur, da erhöhte Körpertemperatur andere Ursachen haben kann und nicht zwingend auf Covid 19 hindeutet.

DER EINGRIFF KANN DURCH SCHONENDERE MASSNAHMEN VERMIEDEN WERDEN

Der letzte Punkt könnte das berechtigte Interesse nach Art 6 Abs 1 lit f DSGVO sein. Dazu muss ein berechtigtes Interesse vorliegen, die Verwirklichung dieses Interesses erforderlich sein und die Interessen, Grundrechte und Grundfreiheiten des Verantwortlichen überwiegen. Wie im vorherigen Punkt kann die Erforderlichkeit nicht bejaht werden, zudem können schonende Maßnahmen zur Vorbeugung der Infizierung getroffen werden, solche wie Anbringen der Hinweisschilder, Tragen des Mund-Nasen-Schutzes, beschränkte Anzahl an Personen usw.

Die der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in Deutschland befand die Einsetzung von elektronischer Messung der Körpertemperatur als unzulässig, da keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten gegeben ist.

DEUTSCHLAND: NUTZUNG VON GOOGLE ANALYTICS BEI UNTERNEHMEN

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder Deutschlands hat eine Stellungnahme zur Anwendung der Google Analytics im nicht öffentlichen Bereich (bei privatwirtschaftlich tätigen Einrichtungen) gegeben. Dieser stellt keine abschließende Beurteilung dar, sondern beschreibt lediglich die datenschutzrechtlichen Mindestanforderungen.

TROTZ GEGENTEILIGER BEHAUPTUNG VERARBEITET GOOGLE PERSONENBEZOGENE DATEN

Problematisch erachtet die Datenschutzaufsichtsbehörde die Behauptung von Google in Analytics-Hilfen, dass die Nutzungsdaten keine personenbezogenen Daten gem DSGVO sind und weist ausdrücklich darauf hin, dass die verarbeiteten Daten personenbezogen sind.

AUFTRAGSVERARBEITUNGSVERTRAG NUR, WENN AUFTRAGGEBER VERANTWORTLICH IST

Nach Meinung der Datenschutzaufsichtsbehörde kann die Einsetzung von Google Analytics nicht unter Auftragsverarbeitung gem Art 28 DSGVO subsumiert werden. Bei der Auftragsverarbeitung hat der Verantwortliche die Zwecke und Mittel der Verarbeitung selbst zu bestimmen.

Dem Auftragsverarbeiter trifft die Pflicht den Weisungen des Verantwortlichen zu folgen. Im Falle von Google Analytics bestimmt nicht der Webseiten-Betreiber allein über die Zwecke und Mittel der Datenverarbeitung, diese werden zum Teil ausschließlich allein von Google bestimmt. Nach der aktuellen EuGH-Rechtsprechung tragen Google und Google Analytics- Anwender gemeinsam die Verantwortung, was den Auftragsverarbeitungsvertrag ausschließt.

EINSETZUNG DIENT NICHT DER VERTRAGSERFÜLLUNG

Der Einsatz von Google Analytics kann nicht auf vertragliche Verhältnisse gem Art 6 Abs 1 lit b DSGVO zurückgeführt werden, da die Einsetzung nicht der Vertragserfüllung dient. Es liegt auch kein überwiegendes Interesse gem Art 6 Abs 1 lit f DSGVO des Webseiten-Betreibers vor, bzw wird das Interesse des Nutzers regelmäßig überwiegen.

RECHTMÄSSIGE VERARBEITUNG NUR MIT EINWILLIGUNG DER NUTZER MÖGLICH

Die einzige rechtmäßige Verarbeitung personenbezogener Daten kann nur durch die wirksame Einwilligung der Webseitennutzer erreicht werden.

Der Nutzer muss vor der Einwilligung klar und deutlich über die Verarbeitung seiner Daten und die Tatsache, dass diese von Google nach Belieben verarbeitet werden und eventuell mit Google-Accounts verknüpft werden, informiert werden.

Zudem muss der Nutzer aktiv (z.B durch Anklicken des Buttons) einwilligen, es darf keine Voreinstellung geben. Die muss zudem freiwillig erfolgen, das ist dann gegeben, wenn der Nutzer eine Wahlmöglichkeit hat die Einwilligung ohne Nachteile zu verweigern.

WIDERRUF MUSS SO UNKOMPLIZIERT WIE EINWILLIGUNG GESTALTET SEIN

Der Widerruf der Einwilligung muss so einfach wie Erteilung der Einwilligung gestaltet sein (Art 7 Abs 3 DSGVO). Es reicht nicht aus den Nutzer auf die Widerrufsmöglichkeit zu verweisen. Das von Google zum Widerruf gedachte Add-On entspricht den Anforderungen des Art 7 Abs 3 DSGVO nicht, weil der Nutzer erst ein Programm runterladen muss um widerrufen zu können.

Zusätzlich zu bereits angesprochenen Maßnahmen sollen Webseiten-Betreiber mit Google Analytics durch die Einstellungen die Kürzung der IP-Adressen vornehmen. Es stellt eine weitere Maßnahme zum Schutz der Nutzer, führt jedoch nicht zu einer vollständigen Anonymisierung der Daten. Die entsprechende Kürzung der IP-Adressen ist in der Datenschutzerklärung entsprechend zu vermerken.

LG HEIDELBERG: KEIN AUSKUNFTSRECHT AUS BACKUP BEI ZU HOHEM AUFWAND

Im Urteil (Az. 4 O 6/19) des Landesgerichts Heidelberg wurde die Zulässigkeit der Auskunftsverweigerung bei zu hohem Aufwand behandelt.

Beim Kläger handelt es sich um ehemaliges Vorstandsmitglied einer Aktiengesellschaft. In dieser Position war er eineinhalb Jahre tätig. Im März 2013 meldete die AG Insolvenz an und wurde in Folge von einem anderen Unternehmen aufgekauft.

BEI GROSSEN DATENMENGEN KANN DIE KONKRETISIERUNG VERLANGT WERDEN

Der Kläger verlangte von dem Insolvenzverwalter Auskunft über seine personenbezogenen Daten gem Art 15 Abs 1 DSGVO. In seinem Hauptantrag wurde nicht präzisiert auf welche Bereiche bzw Kategorien sich die Auskunft erstrecken soll. In so einem Fall darf der Auskunftspflichtige, der große Mengen an Informationen verarbeitet, vor der Auskunftserteilung die Konkretisierung des Auskunftsbegehrens verlangen (Erwägungsgrund 63 DSGVO). Der Kläger gab später an die Auskunft über die Datenkategorie E-Mail-Korrespondenz im genau bestimmten Zeitraum erhalten zu wollen.

HOHER ZEITLICHER UND FINANZIELLER AUFWAND BEFREIT VON AUSKUNFTSERTEILUNG

Erteilung dieser Information wäre für den Beklagten mit zu großem zeitlichen und finanziellen Aufwand verbunden. Da die E-Mails erst aus dem Backup wiederherstellt und bestimmte Stellen mit Informationen über dritte Personen geschwärzt werden mussten und es sich um große Mengen an E-Mails handelte (10.000), fand das Gerichts eine solche Auskunftserteilung als einen unzumutbaren Aufwand. Die Kosten für die Wiederherstellung und Bearbeitung würden sich, nach Berechnungen des Beklagten, auf 124.000 Euro belaufen.

MÖGLICHKEIT EINER WIEDERHERSTELLUNG IST KEIN UNMITTELBARER ZUGRIFF

Weiters war nicht klar, ob der Beklagte die vorliegenden Daten des Klägers überhaupt im Sinne von Art 15 Abs 1 DSGVO verarbeitet. Das Auskunftsrecht umfasst alle Daten, die beim Verantwortlichen vorhanden sind, jedoch muss keine Auskunft über Daten gegeben werden, die zwar in der Vergangenheit verarbeitet wurden, die jedoch nicht mehr zur Verfügung stehen. Das Gericht sah die Möglichkeit einer Wiederherstellung aus dem Backup als nicht unmittelbares Zugreifen an. Jedoch ist die Auskunft nach Art 15 DSGVO über die Daten aus Backup nicht ausgeschlossen, in solchen Fällen kommt es auf den konkreten Aufwand auf Seiten des Verantwortlichen an.

INTERESSEN DES BEKLAGTEN ÜBERWIEGEN

Das Gericht gab der Klage nicht statt. Das Interesse des Klägers steht in keiner Relation zum Aufwand des Beklagten. Zudem handelt es sich um E-Mails, die neun Jahre zurückliegen. Diese existieren in solcher Form auch nicht mehr und die AG, bei der der Kläger beschäftigt war, wurden von einem anderen Unternehmen aufgekauft.

DER VERARBEITUNGSZWECK LIEGT NACH NEUN JAHREN NICHT MEHR VOR

Fraglich ist in diesem Fall, warum die personenbezogenen Daten des Klägers überhaupt noch vorhanden sind. Zwar kann man auf diese, wie das Gericht Heidelberg erkannte, nicht unmittelbar zugreifen, jedoch sind die Daten nicht anonymisiert und können bei Bedarf jederzeit wiederhergestellt werden. Nach Art 20 Abs 1 DSGVO ist der Verantwortliche verpflichtet die personenbezogenen Daten zu löschen, wenn der Verarbeitungsgrund weggefallen ist. Die E-Mails des Klägers sind neun Jahre alt und sind vermutlich nur für das insolvente Unternehmen relevant gewesen. Daraus kann man schließen, dass der Verarbeitungszweck nicht mehr gegeben ist. Zwar verlangte der Kläger keine Löschung, in solchen Fällen muss der Verantwortliche selbständig tätig werden und die Daten löschen.

ZULÄSSIGKEIT VON „DOPPELGLEISIGKEIT“ BEIM RECHTSSCHUTZ

In der Entscheidung (W274 2214412-1/5E) hat BVwG über die Möglichkeit von mehreren Rechtsschutzmöglichkeiten bei datenschutzrechtlichen Angelegenheiten entschieden.

Anlass dafür war die Beschwerde einer Ärztin, die gegen ein Arztsuchportal mit Bewertungsfunktion der Ärzte bei der Datenschutzbehörde vorgehen wollte, weil sie für die Verarbeitung ihrer Daten keine Zustimmung erteilt hatte.

ZURÜCKWEISUNG WEGEN DER ANHÄNGIGKEIT BEIM HANDELSGERICHT

Ein Problem stellte die zuvor eingebrachte und noch anhängige Klage beim Handelsgericht Wien dar. Auf Grund dieser Tatsache wies die

Datenschutzbehörde die Beschwerde mit der Begründung zurück, dass die selbe Sache nicht gleichzeitig Gegenstand zweier Verfahren bei unterschiedlichen Behörden sein kann.

PARALLELZUSTÄNDIGKEIT IN ÖSTERREICHISCHEM RECHT NUR BEI UNTERSCHIEDLICHEN ASPEKTEN

Das BVwG sah abgeleitet vom Art 77 und Art 79 DSGVO die Möglichkeit gleichzeitiger Inanspruchnahme verwaltungsrechtlicher sowie gerichtlicher Rechtsbehelfe und verwies dabei auf ein frühes Urteil (6 Ob 91/19d) des VwGH. Bei der Verabschiedung der DSGVO hat Österreich sich als einziger Staat mit der Begründung dagegen ausgesprochen, dass durch die Parallelität der Rechtschutzmöglichkeiten sich widersprechende Entscheidungen in derselben Sache entstehen könnten. Diese Überlegungen zeigen die gewollte Doppelgleisigkeit des Rechtsschutzes bei DSGVO durch den Gesetzgeber.

Das Verbot der Parallelzuständigkeit im österreichischen Rechtsystem verpflichtet den Gesetzgeber dazu die Angelegenheiten entweder den Gerichten oder Verwaltungsbehörden zur Gänze zu erteilen, damit es nicht zu Vermischung kommt. Zulässig ist es jedoch einen Lebenssachverhalt unter mehreren Aspekten aufzuspalten, dann wäre die gleichzeitige Entscheidungsmöglichkeit von Gericht und Verwaltungsbehörden zulässig.

DSGVO ERLAUBT DOPPELTE ZUSTÄNDIGKEIT BEIM GLEICHEN SACHVERHALT

Im Umkehrschluss bedeutet es, dass bei datenschutzrechtlichen Angelegenheiten auch dann die Inanspruchnahme von ordentlichen Gerichten und der Datenschutzbehörde möglich ist, wenn es sich um eine Sache mit gleichen Sachverhalten handelt.

KURIOSES & FAMOSES

DNA-MÜSLI MIT FOLGEN

Gesundheit ist in aller Munde. Man muss mehr Sport machen, auf die Ernährung achten, dazu kommen gefühlt wöchentlich neue Ergebnisse von Studien, was man nun alles essen darf. Die Lebensmittel, die gestern noch in den Himmel gehoben wurden, sind auf einmal ungesund. Auch die Unternehmen verpassen keine Möglichkeit und lassen sich immer neue und absurde Ideen einfallen. So die mymuesli GmbH, die sich als ökologisch und nachhaltig etabliert, bietet DNA-Kits an um den Stoffwechseltyp zu ermitteln.

Der Ablauf ist einfach, man macht einen Mundabstrich und schickt den ein. Einige Tage später bekommt man einen Bericht mit Informationen und Auswertungen. Passend auf die Ergebnisse des Tests wird die persönliche Müsli-Mischung zusammengestellt. Da steht dem gesunden und ewigen Leben nichts mehr im Weg.

Es wird der Anschein von Professionalität erzeugt und die Tatsache verharmlost, dass es sich um hochsensible Daten handelt. Anhand von DNA können Schlüsse auf Krankheiten, Veranlagungen und Erbfehler gezogen werden, es können sogar die Verwandtschaftsbeziehungen- und Abstammung ermittelt werden. Es ist ein gefährliches Spiel mit sensiblen Daten, die Wirkung von der auf die DNA abgestimmten Ernährung ist zudem wissenschaftlich nicht belegt.

Die DNA-Tests werden nicht von mymuesli GmbH, sondern in Kooperation mit LykonDX, einem auf DNA-Tests spezialisierten Unternehmen, durchgeführt. Die Datenverarbeitung wird gemäß Art 26 DSGVO gemeinsam ausgeführt, somit sind beiden Unternehmen für die Datenverarbeitung verantwortlich.

In den Datenschutzerklärungen hört sich alles harmlos an, die Testkits werden bei mymuesli GmbH gekauft und nach Durchführung des Tests an die LykonDX geschickt. Nach Auswertung der Ergebnisse bekommt mymuesli GmbH nur Vor- und Nachname, Geschlecht, E-Mail-Adresse, Herkunftsland, die Ergebnisse des Tests in Form des Stoffwechseltyps oder der Blutwerte. Mymuesli GmbH verpflichtet sich in seiner Datenschutzerklärung die personenbezogenen Daten nicht an Dritte weiterzugeben, noch für andere Zwecke zu verwenden.
Bei der Dauer der Speicherung wird nur auf die gesetzlichen Fristen verwiesen, etwa die üblichen handels- und steuerrechtlichen Aufbewahrungsfristen. Dabei haben diese Fristen keine Anwendung bei hochsensiblen Daten wie DNA-Ergebnisse und können nicht damit begründet werden.

LykonDX hat seine eigenen Regeln, was die Datenweitergabe betrifft und führt in seiner Datenschutzerklärung sehr wohl aus, dass die Daten an Dritte, wie Werbepartner, Kreditinstitute oder öffentliche Stellen und Institutionen weitergegeben werden, wenn gesetzliche Verpflichtung oder Einwilligung vorliegt. Das geschieht auch dann, wenn die Dritten ihre Niederlassung außerhalb der EU haben. Die Aufbewahrungsdauer der Daten beträgt 10 Jahre.
Aus datenschutzrechtliche Sicht handelt es sich um ein sehr bedenkliches Angebot, von dem Abstand genommen werden sollte. Auch die Datenschutzerklärungen beider Unternehmen erwecken nach Meinung von ARGE DATEN kein Vertrauen.

https://www.mymuesli.com/aktion/dna-muesli-mix-april-april
https://www.mymuesli.com/datenschutz
https://shop.lykon.de/pages/datenschutzerklarun

SMARTE TOILETTE MIT ANUS-SCAN

Die Gänge zum Arzt sind mühsam und nehmen das kostbarste Gut des 21. Jahrhunderts in Anspruch - die Zeit. Die Vorstellung sich schnell zuhause durchchecken zu lassen erscheint wie die Szene aus einem Science-Fiction Film, doch die Wissenschaft macht es möglich.

Die US-Forscher haben eine smarte Toilette entwickelt, die Kot und Urin analysiert und den Benutzer biometrisch identifiziert. Die ermittelten Daten werden über ein Cloudsystem den Ärzten und Gesundheitseinrichtungen bereitgestellt. Für die Zuordnungen der Daten zu einem bestimmten Patienten ist die Spültaste mit einem Fingerabdruck ausgestattet. Für den Fall, dass die Spültaste jemand anderer betätigen soll, wurde zusätzlich eine Kamera mit Scanfunktion eingebaut, die den Anusabdruck erfasst. Laut Forschern hat jeder Mensch einen einzigartigen Anusabdruck, der, wie der Fingerabdruck, nur einmalig vorkommt.

Sollte die smarte Toilette die Räumlichkeit der Forschungsanstalt verlassen und der Allgemeinheit zugänglich werden, werden sich massive datenschutzrechtliche Probleme stellen.

https://med.stanford.edu/news/all-news/2020/04/smart-toilet-monitors-for-signs-of-disease.html

WERDEN SIE MITGLIED DER ARGE DATEN!

ZIELE DER ARGE DATEN

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

MITGLIEDSCHAFT

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

ORDENTLICHES MITGLIED:

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

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

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

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

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

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

FÖRDERNDES MITGLIED:

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

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

LEISTUNGEN DER ARGE DATEN

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

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

ANTRAG AUF MITGLIEDSCHAFT:

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

_____

Zustelladresse:

_____

Telefon: _____

Telefax: _____

Mail: _____

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

ART DER MITGLIEDSCHAFT:

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

_____EUR zutreffendes bitte ankreuzen/ausfüllen

Ort, Datum: _____

Rechtsgültige Unterschrift/Stempel:

_____

PRIVACY POLICY

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

AUSZUG AUS DEN VEREINSSTATUTEN:

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

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

Mittel zur Erreichung des Vereinszwecks (§ 3):

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

WEITERE ANGABEN ZUR MITGLIEDSCHAFT:

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

AnsprechpartnerIn für die ARGE DATEN:

_____

Adresse:

_____

Telefon:

_____

Alle Informationssendungen der ARGE DATEN sollen an folgende Adresse erfolgen:

_____

_____

_____

Für Fragen der Rechnungslegung ist zuständig:

_____

Adresse:

_____

KENNEN SIE ALLE UNSERE LEISTUNGEN?

Fordern Sie die aktuellen Prospekte und Broschüren an!

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

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

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

DATENSCHUTZSTENOGRAMM 2020/21

15. FEBRUAR 2021
DSB-Entscheidung (2021-0.101.211): Durch die Weitergabe des negativen PCR-Tests liegt keine Verletzung des Rechts an Geheimhaltung vor. Die negativen Tests sind Gesundheitsdaten, die Weitergabe ist jedoch durch Verordnung elektronischer Labormeldungen in das Register anzeigepflichtiger Krankheiten berechtigt. Die Verordnung ist klar und präzise formuliert und entspricht dem Erwägungsgrund 41 DSGVO.
https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20210215_2021_0_101_211_00/DSBT_20210215_2021_0_101_211_00.html

13. FEBRUAR 2021
Behörden nutzen „reCaptcha" von Google bei Impfvoranmeldung. Dabei handelt es sich um einen Google-Dienst, der hilft zu erkennen, ob Formulare von echten Personen oder Computerprogrammen ausgefüllt wurden. Problematisch dabei ist, dass die IP-Adressen in die USA übermittelt werden..
https://futurezone.at/netzpolitik/datenschutz-maengel-bei-corona-impfvoranmeldung/401185225

19. NOVEMBER 2020
DSB-Entscheidung (GZ 2020-0.743.659): Die Wiener Contact-Tracing Verordnung sieht weder klare noch präzise Regeln für die Tragweite und Anwendung dieser Maßnahme vor, weil das nicht den EU Vorschriften entspricht. Zudem ist der Grundsatz von Treu und Glauben verletzt, weil keine hinreichende gesetzliche Regelung vorliegt und die Erhebung der Daten gleichzeitig auf Freiwilligkeit beruht, was für den Betroffenen irreführend ist..
https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20201119_2020_0_743_659_00/DSBT_20201119_2020_0_743_659_00.html

12. NOVEMBER 2020
Entscheidung-Italienische Datenschutzbehörde (web. nr.:9485681): Strafe für Vodafone-Italien in Höhe von 12 Millionen Euro für die rechtswidrige Verarbeitung personenbezogener Daten für Telemarketing. Die Untersuchung wurde aufgrund vieler Beschwerden über die unerwünschte Kontaktaufnahme durch Vodafone und sein Vertriebsnetz eingeleitet. Die Untersuchung ergab vielerlei Verstöße, neben der fehlenden Einwilligung der Kunden wurden auch die leitenden Grundsätze der DSGVO nicht eingehalten.
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9485754

20. OKTOBER 2020
DSB-Entscheidung (GZ 2020-0.550.322): Durch die Videoaufnahme mit dem Smartphone in einer WC-Kabine, verhängte die Datenschutzbehörde eine Strafe in Hohe von 150 Euro. Die Strafe ist aufgrund der persönlichen finanziellen Lage des Beschuldigten so niedrig berechnet worden.
https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20201019_2020_0_550_322_00/DSBT_20201019_2020_0_550_322_00.html

10. OKTOBER 2020
Urteil des LG Köln (28 O 71/20): Die Kontoauszüge wurden von der Bank an die falsche Person verschickt. Dabei handelt es sich um einen Rechtsanwalt, der Betreuer der Mutter der Klägerin war. Nach dem Tod wurde das Konto auf die Klägerin überschrieben. Die Bank verabsäumte die neue Adresse einzutragen. Die Klägerin verlangte 25.000 Schadenersatz, da der Rechtsanwalt im Erbaufteilungsverfahren des verstorbenen Vaters der Klägerin die Gegenseite vertreten hat. Nach Erhalt des Briefes musste die Klägerin sich an die schlimme Zeit erinnern, was sie zu tiefst verletzte und traurig machte. Für die Berechnung und Zuspruch des Schades ist die Art, Schwere, Dauer und Umfang des Verstoßes maßgeblich. Es handelte sich um erstmalige und einmalige Falschzusendung und konnte nicht darlegen, ob der Rechtsanwalt überhaupt Einblick in die Kontoauszüge genommen hat. Deswegen wird der Schadenersatz nicht zugesprochen.
https://openjur.de/u/2306367.html

1. OKTOBER 2020
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: Strafe gegen H&M Hennes & Mauritz Online Shop A.B. & Co. KG in Höhe von 35 Millionen Euro. Seit 2014 sammelte das Unternehmen Informationen über private Umstände der Mitarbeiter. Nach dem Urlaub oder einer-Krankheit wurden „Welcome Back Talk" durchgeführt, dabei wurden die Mitarbeiter über Erlebnisse, Krankheitssymptome und Diagnosen ausgefragt und die erhaltenen Informationen auf einem Netzlaufwerk dauerhaft gespeichert. Dazu kamen auch die Einzel- und Flurgespräche. Zugriff auf die Daten hatten rund 50 Führungskräfte. Aufgeflogen ist es im Oktober 2019 durch einen Konfigurationsfehler, die Daten konnten für mehrere Stunden unternehmensweit eingesehen werden.
https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren

10. AUGUST 2020
DSB-Entscheidung (2020-0.204.456): Der Ehemann der Betroffenen fertigte die Tonbandaufnahmen und What's App Verläufe an um diese im Scheidungsverfahren zu verwenden. Die Betroffene wollte die Auskunft von ihrem noch Ehemann über die gespeicherten Daten erhalten. Dieser erteilte ihr eine Negativauskunft und berief sich auf die Haushaltsausnahme gemäß Art 2 Abs 2 lit c DSGVO. Nach DSB greift in diesem Fall keine Haushaltsausnahme, weil keine Zurechenbarkeit zum privaten Bereich vorliegt. Es kommt auf die persönliche und familiäre Tätigkeit der Person und nicht auf die Person, deren Daten verarbeitet werden an. Sogar die gemischte Verwendung würde zur Anwendung DSGVO führen
https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20200810_2020_0_204_456_00.html

11. MAI 2020
DSB-Entscheidung (DSB-D124.137): Die Versendung eines E-Mails mit Kopie an mehrere andere Empfänger verletzt das Recht auf Geheimhaltung. Der Mitarbeiter einer Universität hatte versehentlich statt das E-Mail an einen einzigen Bewerber für die Professur-Stelle an weitere 55 Bewerber als CC verschickt. Die Tatsache, dass die Daten womöglich im späteren Bewerbungsverlauf veröffentlicht würden (z. B öffentliche Anhörung), ändert nichts am unzulässigen Verarbeitungsvorgang.
https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20200511_2020_0_288_477_00.html

7. APRIL 2020
Beschluss des Finanzgerichts (DE) (II B 82/19): Der Kläger verlangte Auskunft gem Art 15 DSGVO über die von ihm durch das Finanzamt gespeicherten Daten.

Das Finanzamt wendete ein, dass die DSGVO in diesem Fall keine Anwendung findet (Art 2 Abs 2 lit d DSGVO). Das ist dem Kläger bewusst, jedoch kann es nach seiner Meinung kein rechtsfreier Raum sein, da der Kläger der Rechtsbürgerszene zugeschrieben wird und es beim Finanzamt vermerkt ist. Im BDSG findet sich keine Regelung bei welchen Gerichten gerichtlicher Rechtschutz zu suchen ist. Deswegen verwies das Finanzgericht auf die Regelung in der Verwaltungsordnung, wonach alle öffentlich-rechtlichen Streitigkeiten nichtverfassungsrechlicher Art vor Verwaltungsgerichte gehören. Das Finanzgericht verwies die Rechtssache an das zuständige Verwaltungsgericht.
https://www.bundesfinanzhof.de/de/entscheidung/entscheidungen-online/detail/STRE202010111/

5. MÄRZ 2020

Urteil Arbeitsgericht Düsseldorf (9 Ca 6557/18): Der Verantwortliche muss 5000 Eur Schadenersatz an den Betroffenen für die verspätete und lückenhafte Erteilung der Auskunft zahlen. Bei dem Auskunftsrecht handelt es sich um ein bedeutsames Recht. Zudem hielt der Verstoß mehrere Monate an, in der Zeit war der Kläger im Ungewissen über die Datenverarbeitung. Dem Betroffenen ist ein immaterieller Schaden entstanden. Er verlangte den Schadenersatz in Höhe von 12 Monatsgehältern. Das Gericht stellte fest, dass der Verdienst des Betroffenen keine Auswirkung auf die Höhe des Schadens hat. Der Betroffenen hatte nur einen unerheblichen Schaden erlitten, deswegen sprach das Gericht weniger Schadersatz zu, als vom Betroffenen ursprünglich verlangt.
https://openjur.de/u/2202048.html

3. MÄRZ 2020

Niederländische Datenschutzbehörde: Strafe gegen einen Tennisverein in Höhe von 525.000 Euro für den Verkauf der Mitgliederdaten an Sponsoren. Für den Verkauft wurde keine Einwilligung der Betroffenen eingeholt. Der Verein berief sich auf Art 6 Abs 1 lit f DSGVO (berechtigtes Interesse), weil das im Interesse des Vereins ist mehr Einnahmen zu verzeichnen, nachdem die Anzahl der Mitglieder abnahm. Die NL Datenschutzbehörde war anderer Ansicht und stellte fest, dass die Datenweitergabe ohne gesetzliche Grundlage erfolgt ist.
https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fines-tennis-association

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

AUFHEBUNGEN CORONA VO

10. März 2021

Aufhebung des § 1 Z 2 lit. e sowie § 2 der Verordnung des Magistrats der Stadt Wien betreffend Auskunftserteilung für Contact Tracing im Zusammenhang mit Verdachtsfällen von COVID-19 (OGH V 573/2020-16).

9. März 2021

Aufhebung der Wortfolge „sowie von Freizeit- und Sportbetrieben" und die Wortfolge „oder der Benützung von Freizeit- und Sportbetrieben" in § 1 der Verordnung „Vorläufige Maßnahmen zur Verhinderung der Verbreitung von COVID-19" (OGH V 530/2020-11).

10. Dezember 2020

Der § 5 Abs. 1 in Verbindung mit Anlage B, Z 4.2 sowie § 7 Abs. 3, 4 und 6 gesetzwidrig in Verordnung zur Bewältigung der COVID-19 Folgen im Schulwesen für die Schuljahre 2019/20 und 2020/21 (OGH V 436/2020-15).

1. Oktober 2020

Das Wort „angeschlossene" in § 2 Abs 1 Z 12 gesetztwidrig in Vorläufige Maßnahmen zur Verhinderung der Verbreitung von COVID-19 (OGH V 392/2020-12)

1. Oktober 2020

Der § 6 gesetzwidrig in Lockerungen der Maßnahmen, die zur Bekämpfung der Verbreitung von COVID-19 (OGH V 429/2020-10).

1. Oktober 2020

Der § 10 der VO gesetzwidrig in Lockerungen der Maßnahmen, die zur Bekämpfung der Verbreitung von COVID-19 (OGH V 428/2020-10).

1. Oktober 2020

Die Wortfolge „und eine den Mund- und Nasenbereich abdeckende mechanische Schutzvorrichtung zu tragen" in § 1 Abs. 2 in Lockerungen der Maßnahmen, die zur Bekämpfung der Verbreitung von COVID-19 (OGH V 463-647/2020-16).

1. Oktober 2020

Der § 6 Abs. 1 und 4 ergriffenen Maßnahmen gesetzwidrig in Lockerungen der Maßnahmen, die zur Bekämpfung der Verbreitung von COVID-19 (OGH G 272/2020-11).

1. Oktober 2020

Der § 6 Abs. 5 ergriffenen Maßnahmen gesetzwidrig in Lockerungen der Maßnahmen, die zur Bekämpfung der Verbreitung von COVID-19 (OGH G 272/2020-11).

14. Juli 2020

Die §§ 1, 2, 4, 6 wegen dem unmittelbaren Eingriff in die Rechtssphäre gesetzwidrig in Verordnung gemäß § 2 Z 1 des COVID-19-Maßnahmengesetzes (OGH V 363/2020-25).

EXTERNER DATENSCHUTZ-BEAUFTRAGTER GEMÄß DSGVO

Vorteile eines externen Datenschutzbeauftragten
Seit 25. Mai 2018 müssen zahlreiche Einrichtungen (Vereine, 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

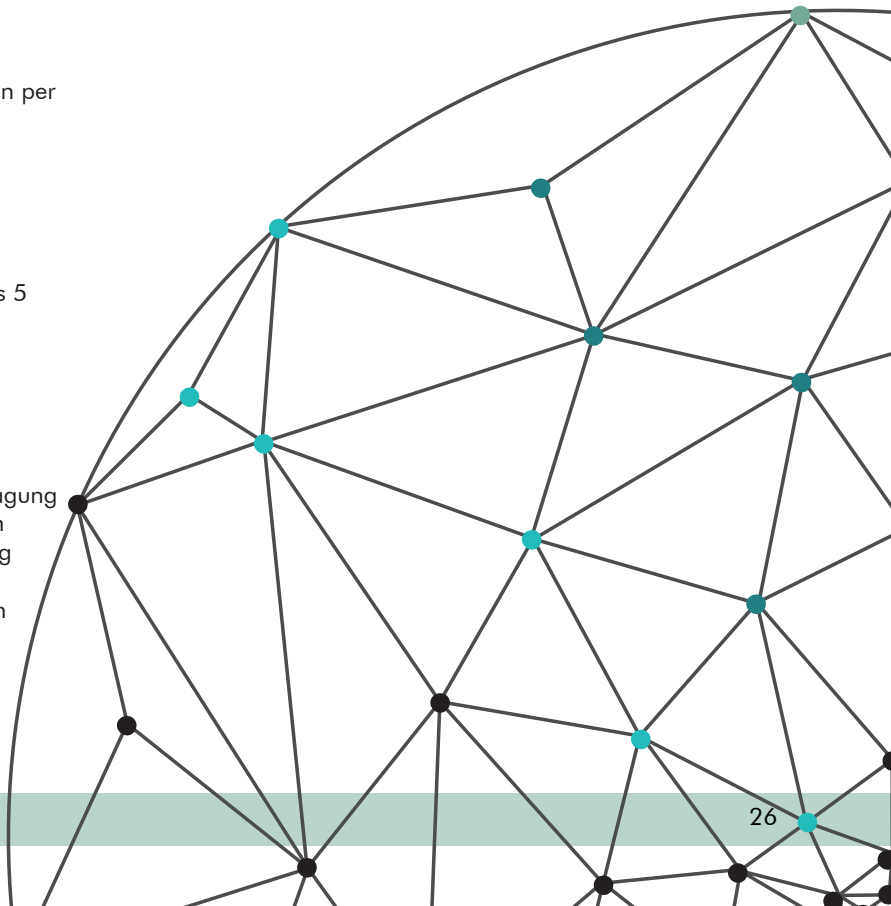
Geeignet für kleine und mittlere Unternehmen mit geringer Zahl an personenbezogenen Datensätzen und geringerr Zahl von Verarbeitungen (max 3)

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)

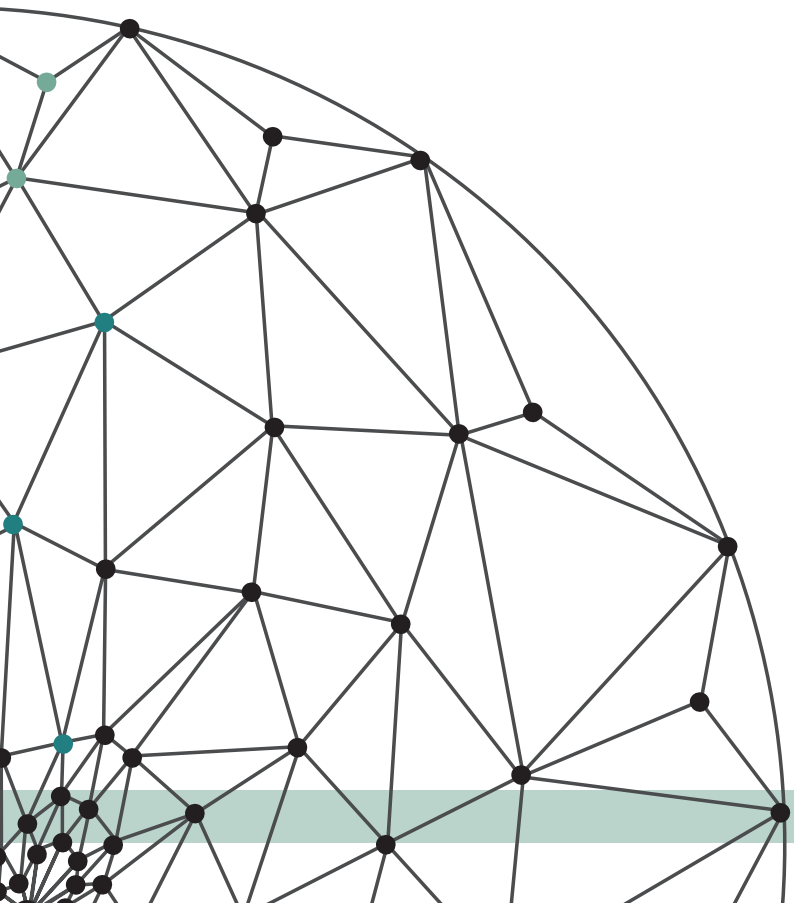


EXTERNER DATENSCHUTZBEAUFTRAGTER - FULL

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

Die redaktionelle Betreuung diesjährigen Jahresberichts erfolgte durch Mag. iur. Julia Komarow und Dr. Hans G. Zeger.

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

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

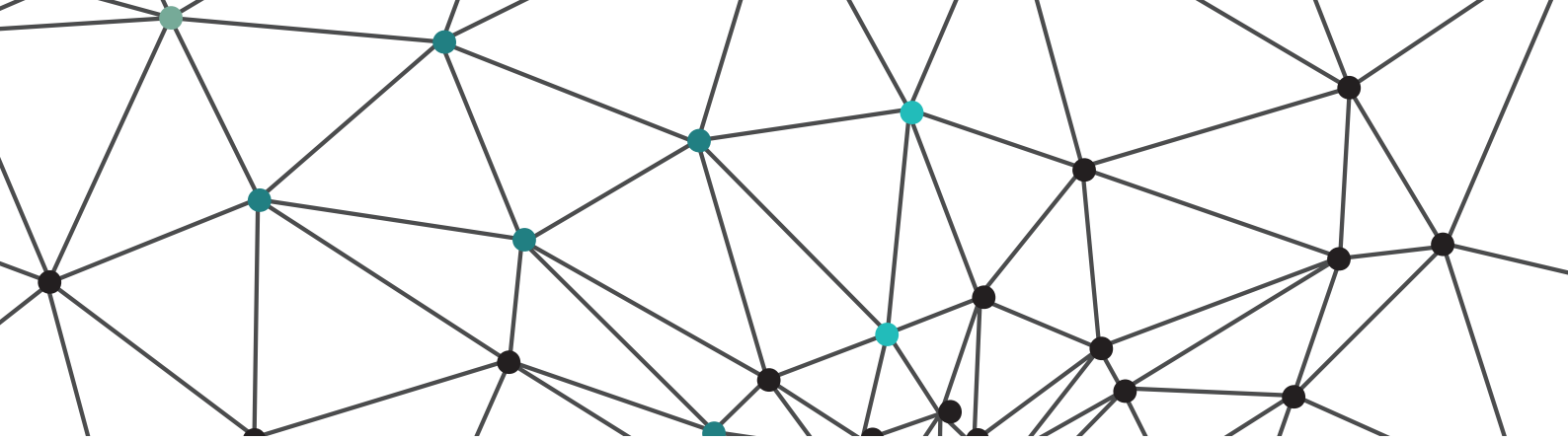
Servicebetrieb zur Abwicklung von Bestellungen und Verrechnung:
e-commerce monitoring GmbH, HG Wien FN 224536 a
http://www.e-monitoring.at

Bildnachweis:
S. 9, 12 siehe Quelle pixbay.com
S. 15, 18 siehe Quelle flickr.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.