ARGE DATEN Privacy Austria

Tätigkeitsbericht 2014

ARGE DATEN
www.argedaten.at

Editorial

2014, das Jahr großer Datenschutzentscheidungen, international standen die EU-weite Aufhebung der Vorratsdatenspeicherung und das richtungsweisende Google-Urteil, beides vom EuGH im Zentrum der Aufmerksamkeit. National standen der Start der neuen Datenschutzbehörde, ELGA-Start, die Aufhebung der Vorratsdatenspeicherung durch den VfGH, die Einführung der zentralen Schülerdatenspeicherung und zahllose Datenschutzentscheidungen der Gerichte im Zentrum der Diskussion.

Den EU-Wahlen im Mai 2014 zum Opfer fiel der geplante Beschluss der EU-Grundverordnung Datenschutz. Noch im März 2014 bestätigte das EU-Parlament die Datenschutzlinie des Parlamentsausschusses LIBE.

Wir erinnern uns, 2012 hatte noch Justizkommissarin Viviane Reding vollmundig angekündigt, ein einheitliches, strenges Datenschutzrecht in Europa zu etablieren, das die Bürger schützt, transatlantische Datenkraken an die Kandare nimmt und Europas Informationsindustrie fördert, quasi eine eierlegende Wollmilchsau.

Die neuen Vorschriften sollten den Menschen mehr Kontrolle über ihre persönlichen Daten geben. Auch sollte sichergestellt werden, dass die gleichen Regeln in allen EU-Mitgliedstaaten gelten, wodurch es für Unternehmen einfacher wird, grenzüberschreitend zu arbeiten.

Der gegenwärtige Diskussionsstand ist ernüchternd, im Rat kämpfen noch immer die Oberdatenschützer aus Deutschland gegen die Datenschutzverweigerer von der britischen Insel um einen „Kompromiss“. Seit den EU-Wahlen im Mai 2014 ist es um die EU-Grundverordnung verdächtig still geworden.

ARGE DATEN berät und hilft

Intensiviert hat sich die Beratungstätigkeit der ARGE DATEN, zahlreiche Beratungen von Unternehmen, Behörden, Medien und Betroffenen konnten zur Verbesserung des Datenschutzes beitragen. Die Leser des Newsletters proftieren direkt von dieser Beratungstätigkeit, viele Auskünfte werden - anonymisiert und verallgemeinert - als „FAQ“-Beitrag veröffentlicht.

Eine besondere Erfolgsgeschichte sind unsere zahlreichen Inhouse-Schulungen und Spezialreferate, bei denen auf die besonderen Bedürfnisse der Teilnehmer eingegangen wird. Unter anderem konnte eine ganze Veranstaltungsreihe für Kriminalpolizisten vereinbart werden.

Hier förderten die Diskussionen im Spannungsfeld von Aufklärungsinteressen und Schutz der Privatsphäre Erstaunliches aus den Abgründen des Innenministeriums zu Tage. Die kriminalpolizeilichen Kompetenzen und Strukturen sind in Österreich nach wie vor so zersplittert, die Ausstattung mit technischen Hilfsmitteln so schlecht, dass sich Täter in Österreich nur freuen können.

Zwischen 38 und 151 Datenanwendungen haben die Polizeidienststellen in Österreich beim DVR registriert. Abhängig in welchem Bundesland man sich aufhält, obwohl im gesamten Bundesgebiet dasselbe Sicherheitspolizeigesetz gelten sollte. Ermittlungsdaten sind auf zahllose Stellen verstreut, die zum Teil eifersüchtig darauf achten, dass andere Stellen nur gefilterten Zugang erhalten.

Beschönigt wird dieses sicherheitspolitische Chaos mit „Datenschutz“. Das Grundrecht Datenschutz wird hier missbraucht und muss - wieder einmal - als Ausrede organisatorischer Missstände und innerministerieller Machtspiele herhalten. So reicht es für Einbruchdiebe etwa in der Perchtoldsdorferstraße bloß die Straßenseite zu wechseln und schon versinken ihre Straftaten im Kompetenzwirrwar zahlloser Polizeidienststellen.

„Eigentlich ist das Innenministerium gar nicht an Verbrechensbekämpfung interessiert, sondern nur an Verkehrsüberwachung. Verbrechensbekämpfung kostet Geld, Verkehrsüberwachung bringt Geld.“ lautete der nüchterne Be-

fund eines teilnehmenden Kriminalisten.

Dem kann der Autor nichts hinzufügen, außer die Aufforderung an das Innenministerium, statt ständig neue Befugnisse zu fordern, endlich für zeitgemäße Strafverfolgungsstrukturen zu sorgen, die die Ausforschung von Tätern erleichtern und unbescholtene Bürger in Frieden leben lassen.

ARGE DATEN bringt Klage gegen Google ein

Die ARGE DATEN unterstützt ihre Mitglieder bei der Löschung persönlicher Daten aus der Google-Suchmaschine. Dazu wurde ein einfaches Antragsformular Online gestellt. Meist funktioniert die Löschung anstandslos, in einem Fall ignorierte Google den Löschungswunsch eines Mitglieds. Im Auftrag der ARGE DATEN hat unser Vorstandsmitglied RA Mag. Michael Krenn Klage gegen Google eingebracht, das Verfahren ist noch anhängig.

2015 - das Internet der Dinge wird allgegenwärtige Realität

Mehrfach angekündigt hat 2014 das Internet der Dinge tatsächlich seine Labornischen verlassen. Erstmals kurven fahrerlose PKWs in Deutschland herum, Drohnen übernehmen die Paketzustellung, smarte Fernsehgeräte übernehmen die lästige Programmauswahl. Ganz besonders praktisch dabei ist die Sprachsteuerung. Wer vor dem Fernseher über Politiker schimpft, bekommt gleich die richtigen News zugeschalten. Aber Vorsicht! Die Sprachdaten werden zentral gesammelt, wer zusehr über bestimmte Personen flucht, der hat die Chance auf ein Live-Action-Erlebnis durch einen Wega-Einsatz wegen gefährlicher Drohung. Praktischer ist wohl die Sprachsteuerung für den, der sich vor dem Fernseher in intimen Aktivitäten versucht. Zu den eigenen Lustschreien werden gleich die richtigen Pornos frei Haus geliefert. Praktisch? Oder? Willkommen in der Welt der statt uns handelnden und entscheidenden Maschinen.

Wie auch immer, die ARGE DATEN ist auf 2015 gut vorbereitet. Auf EU-Ebene haben wir unser Engagement im Rahmen von CEDPO intensiviert (http://www.cedpo.eu/), national werden wir in unserem Engagement für verbesserte Grundrechte, abseits von Hysterie und Paranoia nicht nachlassen und unsere Mitglieder weiterhin in der Durchsetzung der Datenschutzrechte unterstützen, über Datenschutzentwicklungen berichten und vor Fehlentwicklungen warnen.

Erfreulich entwickelt sich auch der Mitgliederstand, auch wenn bei einem so breiten Feld wie Datenschutz unsere finanziellen Mittel knapp, zu knapp bleiben. Wir werden weiterhin den bewährten Weg gehen, unsere fachliche Beratungstätigkeit auf hohem Niveau aufrecht zu erhalten und Verwaltung und Marketing so kostengünstig als möglich zu gestalten.

Unterstützen Sie uns in unseren Anliegen, durch Ihren Mitgliedsbeitrag, durch eine Spende oder durch praktische Mitwirkung bei unseren Veranstaltungen.

Hans G. Zeger, Präsident
ARGE DATEN - Privacy Austria

Inhalt

Tätigkeitsübersicht 2014

ARGE DATEN Privacy Austria

Beispiele aus der Beratungspraxis der ARGE DATEN

- Versandhandel: Registrierung von Datenanwendungen
- Interessensgemeinschaft: Sichtung eMails durch Arbeitgeber
- Bundesdienststelle: Zulässigkeit von Cloud-Computing
- Gemeindedienststelle: Parkraumüberwachung mit Echzeitüberwachung der Parkwächter
- Energiewirtschaft: Beratung zur pdf-Rechnung
- Softwarekonzern: Umgang mit eMails ausgeschiedener Mitarbeiter
- Softwareunternehmen: Umfang der Auskunftspflicht
- Umweltschutzorganisation: Zulässigkeit der Konvertierung von Kontonummern auf BIC-Code durch Dritte
- Fachhochschule: Zulässigkeit von eMail-Werbung
- Handelskonzern: Betriebsvereinbarung zur Verwendung und Protokollierung von Mitarbeiterdaten
- Automobilkonzern: Genehmigung und Betrieb von Dashcams
- Bausparkasse: Einsatz von Google Analytics
- Industrieunternehmen: Verwendung von Pseudonymen
- Industrieunternehmen: Online Meinungsumfrage bei Kunden
- Gesundheitsdienstleister: Einverständniserklärung zum Augenscreening

Anfragen und Auskünfte betrafen folgende Bereiche:
(in Klammern Schwerpunkte)

- **Betrieb / Beruf / Anstellung:** 20% (Facebooknutzung durch Personalabteilung, Bewerberdaten, Internetnutzung durch Mitarbeiter, Zugriff auf E-Mail-Konten, konzernweites Marketing, Betriebsvereinbarungen, Pseudonymisierung von Mitarbeiterdaten)
- **Finanzdienstleister / Privatversicherungen / Auskunftsdienste:** 17% (Auskunft und Löschung von Bonitätsdaten, Kreditanfragen verschlechtern Bonität, Richtigstellung und Verwendung von Konkursdaten)
- **Eingriffe in das Privatleben:** 11% (Google verweigert Löschung persönlicher Daten, UVP-Verfahren veröffentlicht Gesundheitsdaten, Veröffentlichung von Meldedaten)
- **Behörden und Verwaltung:** 9% (Datenverwendung bei Melderegister und Wählerevidenzen, Asylakt geht an AMS)
- **Internet und Telekombetreiber:** 9% (Pflicht zur Vorratsdatenspeicherung, Soziale Netzwerke)
- **Gesundheit und Soziales:** 8% (ELGA-OptOut, Ordinationssoftware verändert Patientendaten, Weitergabe Gesundheitsdaten an AMS)
- **Marketing / Konsumentendaten:** 7% (Einsatz von Kundenkarten, Onlinewerbung, Geschäftsbedingungen privater Online-Handelsplattformen, Fingerprint bei Spielautomaten)
- **weitere Themen:** 19% (Videoüberwachung in Thermen, Ablehnung von Smart Meter, Mikrozensus, Anfertigen Veranstaltungsfotos ohne Zustimmung)

Die „Rising Stars" 2014 waren Datenschutzanfragen zu ELGA, zur Google-Löschung und zu unerwünschten Fotoveröffentlichungen im Internet. Die „Dauerbrenner" sind falsche oder unzulässige Bonitätsdaten, Nutzung von Mitarbeiterdaten, Wählerevidenz, Kundenbindungsprogramme und Mikrozensus.

Öffentlichkeitsarbeit, Informationsdienst

- Web-Service: rund 60.000 Besucher/Monat
- Newsletter: rund 5.000 Abonnenten
- Medienanfragen/-berichte: rund 600
- Mitgliederbetreuung / Rechtshilfe: in ca. 300 Verfahren wurden Mitglieder beraten und vertreten

Veranstaltungen, InHouse Schulungen

Rund 600 Personen besuchten unsere Datenschutzveranstaltungen, 43 Personen absolvierten die ARGE DATEN Ausbildungsreihe zum betrieblichen Datenschutzbeauftragten.

Mehrere hundert Unternehmensmitarbeiter wurden im Rahmen von InHouse Schulungen ausgebildet.

Expertentreff Datenschutz

Themen und Referenten

2014 startete die ARGE DATEN mit einem neuen Schulungs- und Diskussionsformat. Viermal wurde der Expertentreff Datenschutz veranstaltet, an dem betriebliche Datenschützer Praxisbeispiele brachten und Mitarbeiter der ARGE DATEN - natürlich anonymisiert - über aktuelle Beratungsfragen berichteten. Im OPEN SPACE konnten die Teilnehmer spontan Datenschutzfragen zur Diskussion stellen.

Die Termine 2015 der Expertentreffs stehen schon fest:

5. Expertentreff
19. März 2015

6. Expertentreff
20. Mai 2015

7. Expertentreff
29. Juli 2015

8. Expertentreff
25. November 2015

Alle Leser sind eingeladen, sich am Expertentreff zu beteiligen, sei es mit einem Praxisbeitrag oder als Teilnehmer. Vorschläge zu Praxisbeiträgen richten die Leser bitte direkt an: hans.zeger@argedaten.at

Praxisbeiträge aus Betrieben

- **Mag. Sigrun Plattner,**
  T-Mobile Austria GmbH
  Internes Verfahren zur Meldung von Missständen (Whistlblowing)
- **Dr. Evelyn Mittler,**
  General Motors Austria GmbH
  Die Umsetzung von Datenschutzanforderungen in Konzernprojekten
- **Christoph Wenin,**
  REWE International AG
  DVR Meldung, elektronische Personalakte
- **Michael Mrak,**
  Casinos Austria AG
  Wie man mehrere Managementsysteme koordiniert und potentielle Interessenskonflikte vermeidet
- **Maga. Renate Grabinger / Mag. Michael Bartl,** ÖAMTC
  Datenverarbeitung in großen föderal strukturierten ideellen Vereinen
- **Beate Cerny, MSc.,**
  Ammonit EDV Consulting
  Einsatz der Sozialversicherungsnummer
- **Dr. Gregor König,**
  Erste Group Bank AG
  Datenschutzbeauftragter - Die Übernahme der Agenden
- **Benigna Prochaska,**
  Sage GmbH
  Datenwünsche der Konzernmutter - wie darauf reagieren?
- **DI Arash Robubi,**
  KMU Forschung Austria
  Meldungen bei DVR-Online
- **Hans Jürgen Ellinger,**
  I. K. Hofmann GmbH
  Datenschutz und Arbeitskräfteüberlassung

Berichte aus der Beratungspraxis der ARGE DATEN

- **Mag. Jacqueline Kachlyr**
  - Krankenstand und Datenschutz
  - Facebook - Können Facebook-Einträge eine Entlassung rechtfertigen?
- **Philipp Hochstöger**
  - WhatsApp Übernahme: Was ändert sich für Nutzer?
- **Mag. Dr. Hans G. Zeger**
  - Konzern-Marketing und Datenschutz
  - Datenschutz in Matrixorganisationen
  - Globale Verwaltung von Bewerberdaten
  - Auskunftspflichten bei Kundendaten gegenüber Behörden und Privaten
  - Darf eine Unternehmensleitung von Mitarbeitern private Kennungen (E-Card, privater Finanz-Online-Zugang) für betriebliche Aufgaben verlangen?
  - Was ist bei der Anonymisierung von Daten aus Datenschutzsicht zu beachten?
  - Datenschutzrechtliche Verpflichtungen bei der Herstellung von Software
  - Videoattrappen und Veranstaltungsfotos
  - Datenschutz und personalisierte E-Mail-Postfächer
  - Veröffentlichungen von Mitarbeiterdaten
  - Zustimmungserklärungen bei Kundenkarten

Datenschutzthemen 2014

EU-Grundverordnung Datenschutz - bitte warten ...

Kurz vor Weihnachten 2014 hat die Bürgerrechtsorganistion Statewatch ein Dokument zum Stand der Beratungen zur geplanten Datenschutz-Verordnung im EU-Rat ins Netz gestellt. Die italienische Ratspräsidentschaft hatte diese Informationen in einem „Geheimpapier" zusammengefasst.

Das Dokument birgt unliebsame Überraschungen, zahlreiche von Lobbyisten geforderte Ausnahmen dominieren mittlerweile den Entwurf, statt Verbesserungen ist eher von „Verwässerungen" die Rede:

- die Verarbeitung persönlicher Daten für Zwecke des Direktmarketings wird als „legitim" erachtet und soll im Einklang mit der geplanten Verordnung stehen

- selbst das Erstellen von Profilen soll weiter erlaubt sein. Ausgeschlossen sein müssten dabei nur Entscheidungen, „die allein auf einer automatisierten Datenverarbeitung" beruhen und rechtliche Auswirkungen haben, die zu einer „signifikanten" Betroffenheit führen, so der Standpunkt des Rates.

- „Identifizierungsnummern, Standortdaten, Online-Identitätsangaben oder andere spezifische Faktoren" sollen nicht als persönliche Daten angesehen werden, „solange sie ein Individuum nicht identifizieren" oder zu einem solchen Prozess beitragen. Auf das heikle Thema IP-Adressen geht der Rat nicht einmal ein.

„Es besteht die Befürchtung, dass das Datenschutzniveau „hinter das bereits heute geltende Datenschutzniveau zurückfallen könnte", betont der Berichterstatter der Abgeordneten, der Grüne Jan Philipp Albrecht. Trotzdem lobte er, dass zumindest „Bewegung in die Verhandlungen der EU-Mitgliedsstaaten zu kommen scheine".

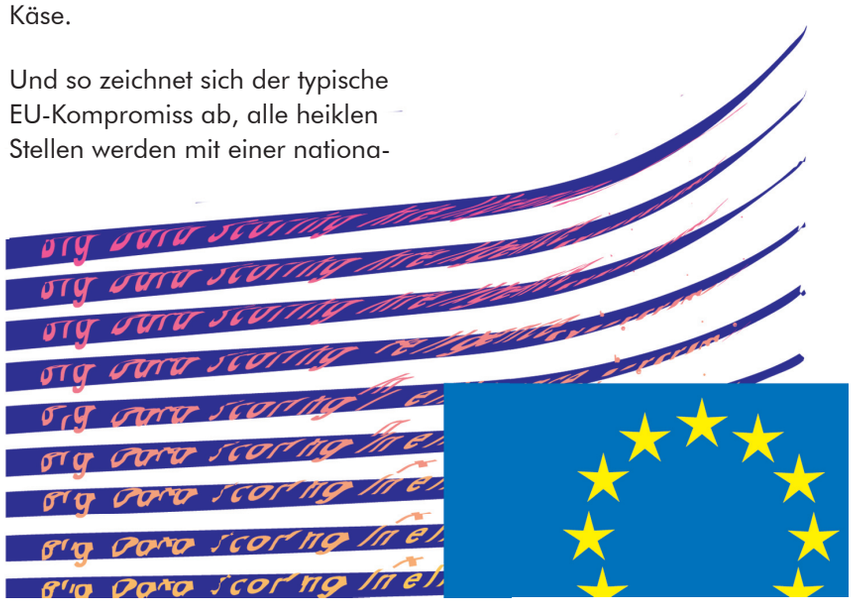
Die neue EU-Kommission hat Null Interesse am Thema Datenschutz, das Thema ist zerredet. Das Parlament hat sich zwar mit seiner bürgerfreundlichen Position festgelegt, ist aber in der EU-Hierarchie noch immer die schwächste Institution.

Ende 2015 soll eine Verordnung beschlossen werden, letzter informell kommunizierter Stand, statt zahlloser delegierender Rechtsakte, die der EU-Kommission weitreichende Datenschutzrechte zugebilligt hätten, werden wohl nationale Ausnahmeklauseln die löbliche Idee eines einheitlichen Datenschutzrechtes durchlöchern wie einen bekannten Schweizer Käse.

Und so zeichnet sich der typische EU-Kompromiss ab, alle heiklen Stellen werden mit einer nationalen Ausstiegsklausel („gemäß nationalen Bestimmungen") versehen. Darunter werden die Zuständigkeit der nationalen Aufsichtsbehörden, die Verpflichtung zum betrieblichen Datenschutzbeauftragten und zahlreiche Melde- und Strafbestimmungen fallen. Wir werden dann ein europaweit „einheitliches" Datenschutzrecht haben, es wird sich aber nicht mehr vom jetzigen - unbefriedigenden - Zustand der unterschiedlichen nationalen Umsetzungen unterscheiden.

Die transatlantischen Internetfirmen wird's freuen und nach TTIP werden nicht einmal diese Standards gelten, denn dann haben internationale Wirtschaftsvereinbarungen Vorrang vor nationalen Grundrechten.

Wir wissen, die EU-Grundverordnung wird kommen, wir wissen nur nicht wann und in welcher Form. Tja, Prognosen sind schwierig, besonders wenn sie die Zukunft betreffen, wer immer diese Weisheit erfunden hat.



2014 Raus aus der Vorratsdatenspeicherung 2015 Rein in die Vorratsdatenspeicherung 2.0?

Eine herbe Niederlage erlebten die Verfechter anlassloser Bürgerüberwachung. Dem Versuch aus dem Verfassungsstaat einen Präventiv- und Alibistaat zu machen, erteilte der EuGH in seinem bemerksenwerten Urteil im April 2014 eine klare deutliche Absage. Bedingungs- und fristlos wurde die gesamte Richtlinie 2006/24/EG zur Vorratsdatenspeicherung aufgehoben. „Zu keinem Zeitpunkt - seit ihrer Verabschiedung 2006 -„, so der EuGH, „bestand eine gültige Rechtsgrundlage für die Vorratsdatenspeicherung". Ein bisher einmaliger Akt. Noch nie hatte der EuGH eine Richtlinie vollständig und fristlos aufgehoben. Üblich waren Teilaufhebungen und Fristen mit Verbesserungsaufträgen an EU-Kommission und EU-Parlament.

Nur drei Monate nach dem eindeutigen EuGH-Urteil hebt der VfGH die österreichischen Vorratsdatenbestimmungen ebenfalls vollständig und ohne Übergangsfrist auf. Gegen den erbitterten Widerstand der österreichischen Bundesregierung, diese hatte bis zuletzt die Regelungen verbissen verteidigt. Im Juli 2014 war Schluss mit der „besonders grundrechtskonformen und gemäßigten Variante" (Eigenlob der Gesetzesautoren) der Vorratsdatenspeicherung.

Auch diese Entscheidung - nicht in der Sache - aber in der für Österreich untypischen Konsequenz kam überraschend. Schon davor hatte sich abgezeichnet, dass die Vorratsdatenspeicherung kein geeignetes Mittel zur Terrorbekämpfung ist. Sowohl die EU-weite Evaluation 2012, als auch die nationalen Erfahrungen zeigten, die Vorratsdatenspeicherung ist perfekt geeignet ab und an einen „Hendeldieb" zu fassen, die Aufklärungsrate mit Vorratsdatenspeicherung kann um etwa 0,001% erhöht werden. Sie versagt aber bei Terrorismus, organisierter Kriminalität und Menschenhandel. Aus nachvollziehbaren Gründen, diese Tätergruppen nutzen elektronische Kommunikationsmittel nur höchst selektiv, die wesentlichen Kontakte finden persönlich oder durch Boten statt.

Selbst Justizminister Brandstetter musste in seinem Vorratsdaten-Bericht eingestehen, dass selbst bei den Alltagsdelikten, bei denen Vorratsdaten zur Aufklärung herangezogen wurden, in den überwiegenden Fällen kein Ermittlungserfolg zu verzeichnen war.

Hans G. Zeger: „Acht Millionen ÖsterreicherInnen unter Generalverdacht zu stellen, ihr Kommunikationsverhalten und ihre Privatsphäre auszuspähen und trotzdem nicht einmal Hendeldiebe zu fassen, das ist eines Rechtsstaats unwürdig. So kann die Argumentation des VfGH kurz zusammengefasst werden."

Die ARGE DATEN hat von Beginn an umfassend über die Entwicklung, die Bedenken aber auch die Erwartungen der Befürworter berichtet, auf http://www.argedaten.at/ kann die Geschichte der Vorratsdatenspeicherung nachgelesen werden.

Vorratsdatenspeicherung 2.0

Glaubt man an den Erfolg der Methode, durch Big-Data-Analysen kriminelle Netzwerke auszuforschen, dann hat uns das FBI schon in den 30er-Jahren vorgezeigt, welche Daten nutzbringender sind, Steuererklärungen, Banktransaktionen, Einkaufs- und Reisedaten.

Wirft man alle diese Daten auf einen großen Haufen und sorgt für eine eindeutige Identifizierung, dann kann das Leben jedes beliebigen Bürgers aufgerollt werden und damit natürlich auch das der Kriminellen. Genau dieses Ziel verfolgt das Projekt Vorratsdatenspeicherung 2.0.

Noch 2015 sollen die Fluggastdaten EU-weit zentral gespeichert werden, die Bankdaten landen sowieso schon in fast allen EU-Ländern in einer zentralen Datenbank, mit eCall wird für den PKW-Verkehr die technische Grundlage zur Aufzeichnung der indivuellen Reisegewohnheiten geschaffen, im öffentlichen Verkehr wird - ganz besonders von realitätsfernen ÖFFI-Fundamentalisten - die umfassende ÖFFI-Card gefordert, die zentral jede Reisebewegung abbucht und verwaltet.
Lücken bei den Reiseaufzeichnungen können durch individualisierte Maut- und Versicherungslösungen geschlossen werden, ebenso durch automatisierte Auswertung der öffentlichen Videoaufzeichnungen. Die erforderlichen Technologien sind schon in den neuen PKWs eingebaut. Mit Smart Meter wird in den nächsten Jahren auch der Energieverbrauch zur Überwachung des Privatlebens erschlossen.

Die bisher größte Überwachungslücke ist - erstaunlicherweise - der private Konsum. Zwar existieren zahllose Kundenkartensysteme, diese sind aber privatrechtlich organisiert und für die Sicherheitsbehörden nur beschränkt zugänglich. Erfolgversprechender ist der skandinavische Ansatz, Bargeld generell zu verbieten.

In Schweden existiert der Slogan „Bargeld ist Diebstahl". Über den Umweg der Bankomat-Transaktionen lässt sich - zentralisiert - zumindest ein grobes Konsumbild gewinnen.

Ich habe nichts zu verbergen - die naive Fehleinschätzung

„Wenn auch nur ein Täter gefasst wird, hat sich der ganze Aufwand gelohnt", ist die bekannte Rechtfertigung, „man habe ja nichts zu verbergen". Eine naive Vorstellung, die sowohl auf einer praktischen, als auch grundrechtlichen Fehleinschätzung beruht.

Aus praktischer Sicht geht es nicht um das Offenlegen oder Verbergen strafrechtlich relevanter Sachverhalte, sondern um den Zwang einer permanenten Rechtfertigung über Sachverhalte, die für sich genommen keinerlei strafrechtliche Komponente haben.

Die gesammelten Verkehrs- und Nutzungsdaten werden als Protokolldaten bezeichnet und sind Abfallprodukte tatsächlicher Geschäftstätigkeiten oder des Bürgerverhaltens. Sie lassen sich, im Gegensatz zu Meinungen oder Umfragen praktisch nicht manipulieren und sind daher qualitativ besonders hochwertig. Umgekehrt haben sie jedoch den Nachteil keine direkten straf- oder sicherheitsrelevanten Informationen zu enthalten.

Ein Telefonat mit Person X, eine Geldtransaktion oder eine Reisebuchung für sich genommen, kann völlig legalen oder auch illegalen Zwecken dienen. Die Daten müssen daher interpretiert werden, das Verhalten eines Bürgers wird von Außen bewertet, kategorisiert und in letzter Konsequenz mit einem Scoringwert belegt.

Das Verhalten eines Bürgers wird mit früheren Erfahrungen und Verhaltensweisen völlig anderer Bürger verglichen und bewertet. Es wird defacto einem Vorurteil unterworfen. Das wirft zahllose praktische Probleme auf, das Reiseverhalten eines Betroffenen, sein Telefonierverhalten oder bestimmte Geldüberweisungen können dem Muster kriminellen Verhaltens entsprechen, ohne tatsächlich einen kriminellen Hintergrund zu haben.

Durch die Verfügbarkeit und zahllosen Interpretationsmöglichkeiten der Daten kommt der Betroffene in die Zwangslage, sich plötzlich für völlig legales Verhalten rechtfertigen zu müssen, nur weil jemand damit kriminelles Verhalten in Verbindung bringt. Der Betroffene muss beweisen, dass sein Verhalten rechtmäßig ist und er muss für Sachverhalte Alibis vorlegen, mit denen er tatsächlich nichts anderes gemeinsam hat, als ein ähnliches Datenmuster.

Die praktische Gefahr der flächendeckenden Vorratssammlungen sind nicht die Daten selbst, sondern deren Interpretationen und der permanente Zwang sich freibeweisen zu müssen. ⏩

mehr unter http://www.argedaten.at/php/cms_monitor.php?q=VORRATSDATENSPEICHERUNG

Um diese Umkehrung der Unschuldsvermutung zum Schuldverdacht und dadurch einen permanenten Rechtfertigungsdruck gegenüber Behörden zu verhindern, sehen alle modernen Verfassungen vor, dass jeder Mensch solange unbeobachtet leben darf, als nicht für das Zusammenleben zwingende Gründe vorliegen, einzelne Informationen offen zu legen.

Das können Einkommensdaten für Steuerzwecke sein, Angaben über ansteckende Krankheiten zur Verhinderung der Ausbreitung und zum Schutz der Volksgesundheit oder eben strafrechtlich relevantes Verhalten zur Ausforschung von Tätern. Liegt keiner dieser Gründe vor, dann dürfen Daten weder verwendet, noch auf Vorrat aufgehoben werden. Die Möglichkeit, es könnte in Zukunft interessant sein, das Leben eines Bürgers aufzurollen, entspricht zwar den Phantasien von Diktatoren, nicht aber einem modernen Verfassungsstaat.

Eine Konsequenz dieses Grundrechtsanspruchs ist, dass einzelne Delikte nicht aufgeklärt und einzelne Täter nicht ausgeforscht werden können. Eine andere Konsequenz ist aber auch, dass sich in einem Klima des Schutzes von Geschäftsgeheimnissen und Privatleben, Wirtschaft und soziales Zusammenleben besser entwickeln, neue Ideen und Kreativität gedeihen können und in Summe der Wohlstand für alle gefördert wird. Eine Gesellschaft, die auf Freiräume für Neues, auf beobachtungsfreie Zonen verzichtet, hat sich in letzter Konsequenz selbst aufgegeben und verwaltet nur mehr noch den erreichten Wohlstand, bis zum völligen Verschwinden.

DATENSCHUTZ-STENOGRAMM 2014

- **Richtungsweisendes EuGH-Urteil zu Suchmaschinen**
- **ARGE DATEN veröffentlicht Musterbrief zur Google-Löschung**
- **ARGE DATEN bringt für Mitglied Löschungsklage gegen Google ein**
- **EuGH erklärt Richtlinie RL 2006/24 zur Vorratsdatenspeicherung für ungültig**
- **Vorratsdatenspeicherung wird vom VfGH auch in Österreich ersatzlos aufgehoben**
- **ARGE DATEN hilft beim Opt-Out aus ELGA**
- **ELGA Fehlstart wird Fall für Volksanwalt**
- **EU-Parlament bestätigt kritische Datenschutzposition des Abgeordneten Jan Philip Albrecht**
- **EU-Grundverordnung Datenschutz lässt wegen EU-Wahl weiter auf sich warten**
- **EU-Parlament fordert Entflechtung von Suchdiensten und anderen Internetangeboten der Firmen**
- **Facebook treibt ihre Vision vom gläsernen User weiter - Max Schrems startet Sammelklage gegen Facebook**
- **Diskussion um neue Datenschutzkonzepte im Zeitalter der Gratisdienste beginnt**
- **personenauskunft.at stellt nach ARGE DATEN Berichterstattung Auskunftsdienst über Privatpersonen ein**
- **OGH beschränkt Anfertigung und Nutzung von Personen-Bildern**
- **SmartTV, SmartCar und SmartMeter, 2014 beginnt das Internet der Dinge unser Alltagsleben zu durchdringen**

EuGH-Urteil C-131/12 stellt fest - Google ist Datenverarbeiter im Sinne der Datenschutzrichtlinie

Mit dem Urteil C-131/12 hat der Europäische Gerichtshof wesentliche Klarstellungen zu Suchmaschinenbetreibern getroffen und damit die Position bestärkt, die von der ARGE DATEN seit 15 Jahren vertreten wird: Suchmaschinen sind wie klassische Datenverarbeitungen organisiert und fallen vollständig unter den Anwendungsbereich der EG-Richtlinie Datenschutz 95/46/EG (http://www.argedaten.at/recht/eu.htm). Für die ARGE DATEN überraschend war, dass die EU 15 Jahre für diese Einsicht benötigte.

Die Ausgangssituation ist bekannt: Ein spanischer Bürger hatte die nationale Datenschutzkommission mit einer Beschwerde gegen eine spanische Tageszeitung sowie „Google inc" und deren spanische Tochtergesellschaft angerufen. Bei Eingabe seines Namens in die Suchmaschine des Google-Konzerns wurden den Internetnutzern Links zu zwei Seiten einer Tageszeitung aus 1998 angezeigt, die eine Anzeige enthielten, in der unter Nennung seines Namens auf die Versteigerung eines Grundstücks hingewiesen wurde.

Der Spanier verlangte die Löschung der Daten, gegen die Google-Gesellschaften war der Beschwerde stattgegeben worden. Google klagte gegen diese Entscheidung, die Sache wurde dem EuGH als „Vorabentscheidungsverfahren" zur Interpretation der EU Datenschutzrichtllinie vorgelegt.

„Vorabentscheidungsverfahren" des EuGH nach Google-Klage

Positiv ist zu bewerten, dass sich der EuGH nicht auf das „Versteckspiel" von Google hinsichtlich der Anwendbarkeit der Richtlinie eingelassen hat. Da Google Spain in Spanien effektiv tätig ist, ist die Datenschutz-Richtlinie auf Google anzuwenden.

Die strittige Frage war, ob überhaupt eine personenbezogen Verarbeitung von Daten vorliegt. Es ist unstreitig, dass sich unter den Daten, die von den Suchmaschinen gefunden, indexiert, gespeichert und den Nutzern zur Verfügung gestellt werden, auch „personenbezogene Daten" befinden. Indem der Suchdienst das Internet automatisch, kontinuierlich und systematisch auf die dort veröffentlichten Informationen durchforstet, „erhebt" der Betreiber personenbezogene Daten, die er dann mit seinen Indexierprogrammen „ausliest", „speichert" und „organisiert", auf seinen Servern „aufbewahrt" und gegebenenfalls in Form von Ergebnislisten an seine Nutzer „weitergibt".

Besonderen Wert legt der EuGH darauf, dass die Nutzer der Suchmaschinen mit der Ergebnisliste einen strukturierten Überblick über die zu der betreffenden Person im Internet zu findenden Informationen erhalten, anhand dessen sie ein mehr oder weniger detailliertes Profil der Person erstellen können. Dieser Umstand könne zu einer erheblichen Beeinträchtigung der Persönlichkeitsrechte führen. Der EuGH sieht eine Interessenabwägung für notwendig an: Das Informationsrecht Dritter und die wirtschaftlichen Interessen des Betreibers seien mit dem Schutz der Persönlichkeitsrechte abzuwägen.

Ein Löschen jeglicher Daten je nach Lust und Laune des Betroffenen hat der EuGH nicht judiziert. Dass es keine klaren Leitlinien gibt - wie Kritiker betonen - ist richtig, aber nicht überraschend: Derartige Konstellationen sind immer Abwägungen im Einzelfall für die es kein Generalrezept geben kann.

Grundsätzlich gilt:
a.) je „schädlicher" und negativer die Information für einen Betroffenen objektiv sein kann, desto eher wird ein Löschungsanspruch bestehen
b.) je geringer der objektive Informationswert für Dritte ist, desto eher wird ein Löschungsanspruch bestehen - insbesondere bei veralteten Daten werden die Chancen höher sein.
c.) Besonderes Augenmerk verdienen Informationen dann, wenn sie sich überhaupt erst aus den Inhalten verschiedener Websites auf Basis des Suchresultats ergeben.

ARGE DATEN unterstützt bei Löschung aus Suchmaschinen - Klage gegen Google eingebracht

Mindestens 100.000 ÖsterreicherInnen sind direkt von veralteten, irreführenden oder fehlerhaften Suchmaschineneinträgen betroffen. Für die Betroffenen hat dieses Urteil die Konsequenz, dass sie sich aus der Google-Suchmaschine und auch aus allen anderen vergleichbaren Such- und Listensystemen löschen lassen können.

Das Urteil geht sogar noch weiter, es ist Betroffenen möglich, vorbeugend einen Widerspruch bei einem Suchmaschinen-Betreiber zu

hinterlegen, dass für die Zukunft keine persönlichen Daten zu seiner Person verarbeitet werden.

Auf Grund des EuGH-Urteils besteht dieser Löschungsanspruch direkt gegenüber dem Suchmaschinen-Betreiber, aber auch gegenüber seinen Tochterunternehmen, die im Bereich der EU ihren Sitz haben. Konkret bei Google wären das Google Inc, USA und Google Austria, Wien.

Die ARGE DATEN hat ein Musterschreiben zur Datenlöschung entwickelt und unterstützt ihre Mitglieder bei Löschungsverweigerung. Sollte eine Löschung nicht wunschgemäß ablaufen, dann wird die ARGE DATEN Betroffene in Musterverfahren vertreten. Ende 2014 wurde von RA Mag. Michael Krenn im Auftrag der ARGE DATEN die erste Klage gegen Google eingebracht.

ELGA - nach Fehlstart 2014, droht 2015 das Chaos?

Erhebliche Aufregung verursachte 2014 ELGA, Österreichs Variante der elektronischen Gesundheitsakte. Was für die einen die Lösung aller gesundheitspolitischen Probleme darstellt, ist für die anderen ein administratives Monster, das nicht zur Verbesserung der Gesundheit beiträgt, sondern bestehende Misswirtschaft teuer verwaltet.

Begonnen hat ELGA am 1.1.2014 mit einem kapitalen Fehlstart. Die einzige Funktion von ELGA war die Möglicheit sich abzumelden („OptOut“). Dazu hatte sich das Gesundheitsministerium eine komplizierte und letztlich nicht gesetzeskonforme Prozedur ausgedacht.

Schon in den ersten Tagen wollten sich Zehntausende abmelden, was zum Zusammenbruch des Systems führte. Manche Betroffene mussten acht(!!) Monate warten, bis ihre Abmeldung akzeptiert wurde.

Die ARGE DATEN ist Anfang 2014 in die Bresche gesprungen und hat ein einfaches Widerspruchsformular entwickelt, das sowohl den Betroffenen, als auch der Widerspruchsstelle des Gesundheitsministeriums die Arbeit erleichterte (http://ftp.freenet.at/privacy/muster/elga-optout.pdf). Mehrere zehntausend Betroffene haben sich mit Hilfe dieses Formulars abgemeldet.

ELGA Widerspruch („Opt-Out“) wird Fall für Volksanwalt!

Zehntausende hatten sich gegen die ELGA-Gesundheits-Vorratsspeicherung ausgesprochen, ihre Widerspruchs- und Informationsrechte wurden jedoch ignoriert. Gesundheitsminister und Hauptverband waren mit der Zahl der Widersprüche völlig überfordert. Die Spekulation von Gesundheitsminister Stöger war nicht aufgegangen: Alle Bürger würden sich mit der Gesundheits-Vorratsspeicherung ELGA zwangsbeglücken lassen und sich dann aus Bequemlichkeit nicht abmelden.

Weil Zehntausende noch nach Wochen vergeblich auf die Bestätigung des Widerspruchs warten, hat der Obmann der ARGE DATEN im Februar 2014 die Volksanwaltschaft eingeschaltet. Danach kam es zumindest in einigen Fällen zur beschleunigten Bearbeitung, Tausende warten aber immer noch auf die Bestätigung ihrer Abmeldung.

Mittlerweile haben mehr als 200.000 Menschen den beschwerlichen Opt-Out-Weg gewählt, bei einem Volksbegehren wäre das ein höchst respektables Ergebnis.

ELGA ist datenschutzrechtlich ein Risikopatient

Datenschutzrechtlich an ELGA ist bedenklich, dass es vom Prinzip der freiwilligen medizinischen Behandlung mit Zustimmung des Patienten abgeht und zur zwangsweise verordneten Gesundheitsleistung wird.

Die ARGE DATEN hat daher von Beginn an festgehalten, dass sie ein elektronisches Gesundheitsinformationssystem begrüßt, das Patienten und Ärzte in der medizinischen Betreuung unterstützt. Ein derartiges System muss jedoch so offensichtliche Vorteile haben, dass alle Beteiligten es gern und freiwillig nutzen.

Faktum ist jedoch, dass über ELGA zwar seit 2006 spekuliert wird, zahllose „Konzepte“ entwickelt wurden, aber bis heute keine praxistauglichen Strukturen geschaffen wurden. Es gibt weder Modellanwendungen, damit Patienten und Ärzte die Praxistauglichkeit prüfen können, noch gibt es eine letztver-

antwortliche Stelle für den sicheren Betrieb. Es gibt keine prüfbaren Sicherheitslösungen, nicht einmal besteht Klarheit, welche Daten in welcher Form im System landen sollen.

Schon die Idee sensible Gesundheitsinformationen als „Akt" zu verwalten, zeigt wie praxisfern und bürokratisch die ELGA-Befürworter agieren. Moderne Hilfsmittel der Medizin, wie Telemedizin, Echtzeitverarbeitung, Datenanalyse und Termin- und Leistungskoordination können durch den ELGAkt nicht geleistet werden. Österreich hinkt der internationalen eHealth-Entwicklung um gut 10-20 Jahre nach.

2015 droht das ELGA-Chaos

Mit 1.1.2015 hätte ELGA in allen Landesspitälern starten sollen, landesfürstliche Kleinkariertheit verhinderte jedoch diesen Start. Nunmehr sollen sich ab Ende 2015 jene Spitäler an ELGA beteiligen, die das wollen. Und zwar, glaubt man den Aussagen der Gesundheitsministerin, in der Form wie sie wollen. Damit geht der letzte Sinn von ELGA, einheitliche Informationsstrukturen zu schaffen, verloren. De facto werden Bundesländer-, wenn nicht sogar Spitals-ELGAs entstehen, bei denen Informationen nicht vergleichbar sind.

Solange die fundamentalen Nutzungsfragen zu ELGA nicht geklärt sind, gibt die ARGE DATEN die Empfehlung ab, zur Sicherheit nicht daran teilzunehmen und „OptOut" zu wählen. Details zu ELGA finden sich unter: http://www.argedaten.at/php/cms_monitor.php?q=E-CARD

personen-auskunft.at

Ein datenschutzrechtlicher Dauerbrenner sind die Aktivitäten der Wirtschaftsauskunftsbüros und der Inkassodienste. Mitte 2014 wurden wir auf personenauskunft.at aufmerksam gemacht. Ein Unternehmen, das unter verschiedenen Namen und Webseitenbezeichnungen auftrat erklärte vollmundig:

„Als Experten für internationale Firmeninformationen liefern wir diskret, kompetent und schnell Handelsregisterauszüge, Firmen- und Bonitätsauskünfte, sowie Informationen aus dem Melderegister. Handelsregister, Firmenauskunft, Firmen-Sofortauskunft, Melderegister."

Zu den Privatpersonen wurde noch nachgelegt: „Mit unserer Personenauskunft erhalten Sie einen Überblick über die Bonität zu über 7 Mio. Privatpersonen in Österreich." und „Überprüfen Sie die wirtschaftliche Situation Ihres neuen Mitarbeiters, Mieters, Käufers oder Partners. OBJEKTIV - ANSCHAULICH - SOFORT"

Dürfen die das, fragten sich nicht nur unsere Mitglieder. Eine Recherche beim DVR ergab, das Unternehmen hatte keinerlei Datenverarbeitung für Bonitätsauskünfte gemeldet. Laut Info der WKO waren auch keine geeigneten Gewerbeberechtigungen gemeldet.

Die ARGE DATEN entschloss sich im Rahmen des Ombudsmannverfahrens die Datenschutzbehörde anzurufen. In einer verworrenen Stellungnahme rechtfertigte sich der Geschäftsführer des Unternehmens, er habe gar keine Personendaten, sondern sei bloß Vermittler der Firma Bisnode. Da aus den Ausführungen nicht erkennbar war, welche Bisnode-Firma tatsächlich gemeint war, wurde von der Datenschutzbehörde amtswegig ein weiteres Prüfverfahren eröffnet.

Der dubiose und nicht regulierte Markt der Bonitäts- und Scoringauskünfte über Privatpersonen ruft laufend Glücksritter auf den Plan, die versuchen mit der wirtschaftlichen Not von Menschen schnelles Geld zu machen. Zum schlimmsten Fall, ein Auskunftsdienst, der illegal die Exekutionsdaten der Justiz verkaufte, wurde 2014 vorläufig ein Schlussstrich gezogen. Einer der Hauptakteure landete hinter Gittern, ironischerweise nicht wegen Datenmissbrauch, sondern wegen Kinderpornographie.

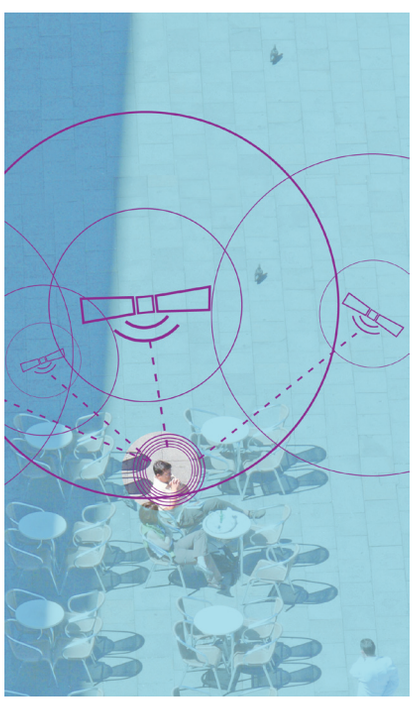
In zahllosen Beratungsfällen mussten wir auch 2014 feststellen, dass falsche Bonitätsdaten verwendet werden, Daten falschen Personen zugeordnet werden und falsche Schlüsse gezogen werden. Zum Schaden der Betroffenen, aber auch zum Schaden der Wirtschaft, die korrekte Daten über Zahlungsunfähige und Zahlungsunwillige benötigt, aber keine fehlerhaften Daten, die nützliche Geschäftsabschlüsse verhindern.

Leider ist seit 2010 die Politik säumig und weiterhin nicht bereit, dem Auskunftsmarkt klare Vorgaben zu machen, welche Bonitätsdaten rechtmäßigerweise verwendet werden dürfen. Ein Säumnis, das sowohl den Betroffenen, als auch der kreditgebenden Wirtschaft, den Banken, Versandhändlern, Telekomfirmen, Hausverwaltern und Energieversorgern schadet.

Die ARGE DATEN wird auch 2015 weiter dranbleiben und bei jedem noch so schläfrigen zuständigen Politiker die Reorganisation der

Wirtschaftsauskunftsdienste einfordern.

Ausführliche Informationen zum Schutz vor rechtswidrig verabeiteten Bonitätsdaten finden sich unter: http://www.argedaten.at/php/cms_monitor.php?q=BONITAET Zu Personenauskunft.at gibt es auch eine gute Nachricht: kurz nach unserer Berichterstattung wurde die Website vom Netz genommen. Wir hoffen, dass es so bleibt.



Schüler sind zum Verwalten da

„Nicht für die Schule, sondern für's leben lernen wir", ist ein bekannter Kalenderspruch der Erzieher. Faktum ist jedoch in Österreichs Bildungssystem, in der Schule lernen die Schüler, dass Bürger bloß Datenlieferanten einer ineffizienten Verwaltung zu sein haben.

Mitte 2014 wurde vom Unterrichtsministerium der Plan bekannt gegeben, künftig das gesamte Schulgeschehen in zentralen Servern zu verwalten (inklusive dem Klassenbuch, das nunmehr elektronisch geführt wird), mit weitreichenden Konsequenzen. Verschwanden früher situative Einträge im Klassenbuch am Ende des Jahres im Keller der Schule und niemand interessierte sich dafür, stehen diese Einträge nun bis zu 60 Jahre nach Schulabschluss zur Auswertung bereit! Schulvorfälle, Betragensnoten, disziplinäre Verwarnungen, Klassenbuchverweise und Schulnoten werden künftig noch zu einem Zeitpunkt personenbezogen abrufbar sein, zu dem der betroffene Schüler gar nicht mehr lebt.

Pädagogisches Geschehen wird zum Verwaltungsakt degradiert, wer das Pech hat als Schüler einem hilflosen Lehrer ausgeliefert zu sein, muss mit zahlreichen Einträgen in diesem Zentralsystem und späteren Nachteilen rechnen.

Übertragen wurde der Auftrag der Grazer bit media, seit Jahren eine Art Haus- und Hoflieferant für das Unterrichtsministerium. Auffällig bei dieser Gesellschaft ist ein unglaublich komplexes Firmennetzwerk mit den immergleichen beteiligten Personen, die in verschiedensten Funktionen einmal als Inhaber, als Gesellschafter, als Geschäftsführer, Aufsichtsrat, Beirat oder einfache Mitarbeiter aufscheinen.

Angesichts der früheren Datenpannen bei BIFIE und Co, die aktuellen Probleme mit den Servern der Zentralmatura und den Begehrlichkeiten der Politik, integrationsunwillige Schüler auszuforschen ein beängstigendes Szenario. In Großbritannien werden schon aus den Schulaufzeichnungen notorische Schwänzer extrahiert und die Daten den Sicherheitsbehörden übergeben. Denn - so die entwaffnende Logik - wer sich als Kind nicht an Schulregeln hält, bricht später auch vermehrt das Strafrecht.

Macht dieses Beispiel Schule, dann könnte sich in einem Land wie Österreich, mit ausgeprägtem Registerwahn (O-Ton Jesionek) ein schier endloses Betätigungsfeld ergeben: Eltern, die Ladungen der Lehrer nicht folgen werden ans Finanzministerium gemeldet, damit die Kinderbeihilfe gestoppt wird, an das AMS, um zu prüfen ob sie Arbeitslose sind und zum Gang zum Lehrer verpflichtet werden könnten. Meldet sich ein Schüler krank, könnten die Daten gleich mit den Krankmeldungen bei der Sozialversicherung abgeglichen werden, gibt der Schüler einen Trauerfall bekannt, könnte der Abgleich mit dem zentralen Personenstandregister erfolgen, gibt es disziplinäre Probleme, dann wäre der automatisierte Datenabgleich mit dem Jugendamt möglich.

Auch die „Kommunikation" mit den Eltern könnte intensiviert werden: zwei Jugendliche werden beim Schmusen am Schulhof beobachtet, der elektronische Klassenbucheintrag verschickt automatisiert ein SMS an die betroffenen Eltern. Gibt es zu viele Schmuse-Einträge, dann könnte auch noch eine Flittchendatenbank angelegt werden.

Der Fantasie sind keine Grenzen gesetzt und - wie die Erfahrung mit ähnlichen Instrumenten zeigt - werden sie früher oder später auch umgesetzt.

Freilich alles auf streng gesetzlicher Grundlage, nicht schon 2015, dann vielleicht 2016 oder als besonderes Wahlzuckerl 2018.

Verwendung von Bild- und Videodaten

Einen Beratungsschwerpunkt stellt seit Jahren die Nutzung von Bild- und Videodaten dar. Hier ziehen Gesetzgebung und Rechtssprechung sehr enge Grenzen, die im letzten Jahr weiter verschärft wurden.

Das Anfertigen und Veröffentlichen von Bildern steht immer im Spannungsfeld der Grundrechte Freiheit der Berichterstattung, des Eigentumsschutzes und des Schutzes der Privatsphäre. Bei jeder Bild- oder Videoaufnahme sind diese drei Interessen abzuwägen, in vielen Fällen ist eine Einzelfallentscheidung erforderlich.

Die ARGE DATEN hat unter: http://www.argedaten.at/php/cms_monitor.php?q=VIDEO umfangreiche Materialen zusammen gestellt, folgende Beschränkungen sind zu beachten:

- unzulässig ist die Überwachung eines Nachbarn oder des öffentlichen Bereichs (etwa eine Wohnstraße oder der Gehsteig vor dem Haus)
- unzulässig ist es auch den Anschein der Überwachung zu erwecken (Videoattrappen)
- unzulässig ist die Überwachung der Wohnungstür eines Mieters durch einen anderen Mieter oder den Vermieter
- unzulässig ist die Veröffentlichung von Mitarbeiterfotos ohne ausdrückliche Zustimmung
- unzulässig ist die Veröffentlichung von Fotos von Privatpersonen ohne deren Zustimmung, auch wenn sie im öfffentlichen Raum aufgenommen wurden
- unzulässig ist die Veröffentlichung von Fotos von Organen (z.B. Polizisten) bei Ausübung ihres Dienstes
- unzulässig ist schon das Anfertigen von Fotos von Personen ohne nachvollziehbaren Grund („just for fun")
- unzulässig ist auch die Aufnahme eines Toten ohne Zustimmung der Angehörigen
- unzulässig ist der Einsatz von Dashcams oder Helmkameras zur permanenten Dokumentation des Verkehrsgeschehens und zur eigenen Absicherung

Für alle anderen Fälle gilt die Interessensabwägung unter Berücksichtigung aller Grundrechte.

Je suis Charlie - feige Mörder erreichen einfach ihre Ziele

Die (Datenschutz-)Konsequenzen aus den feigen Mordanschlägen in Paris Anfang des Jahres werden 2015 die grundrechtliche Diskussion bestimmen.

Fassen wir die Fakten zusammen: Zwei Tätern gelingt es in die Redaktion eines schon früher bedrohtes Satiremagazin einzudringen und mehrere Menschen zu töten, ein weiterer Täter verursacht in einem explizit jüdischen Supermarkt ein Massaker. Beides geschieht in Frankreich, beides zeitlich nahe beisammen, beides mit erscheckender Grausamkeit durchgeführt. Beides in einem Land mit hochgerüstetem Polizeiapparat, einem der weltweit größten Geheimdienste, vernetzt mit allen US-Diensten, in einem Land mit Vorratsdatenspeicherung, die Redaktion war von Polizisten bewacht, allen jüdischen Einrichtungen wurde - zumindest offiziell - besondere sicherheitspolitische Aufmerksamkeit gewidmet.

Wer nun eine Evaluation der Arbeit der Sicherheitsbehörden erwartete, wer Aufklärung erwartete, warum trotz der sicherheitstechnischen Hochrüstung derartige Anschläge möglich sind, der muss sich als politischer Naivling bezeichnen lassen.

Routinemäßig wurden die Empörungsrituale angeworfen, man solidarisiere sich mit den Opfern, man lasse sich nicht von Terroristen die Grundrechte zerstören und man werde besonnen, aber energisch reagieren. Doch schon am Tag danach gewinnt die Sicherheitsparanoia Oberhand, die Vorratsdatenspeicherung soll wieder eingeführt werden, die Fluggastdatenspeicherung im Eilzugstempo beschlossen, das Internet stärker überwacht werden.

Und Europas Spitzenpolitiker sind sich nicht zu primitiv die große Pariser Trauerkundgebung Mitte Jänner 2015 für ihre eigene schäbige Inszenierung zu missbrauchen. Arm in Arm wandern sie, abgeschottet und abgehoben vom Rest der Welt durch eine Pariser Seitengasse, weitab von der eigentlichen Kundgebung und lassen sich so fotografieren, als ob sie mittendrin wären. Selten zuvor wurde das Auseinanderklaffen der politischen Kaste und der Lebens-Realität der Menschen so drastisch dokumentiert.

Für die Beschränkung der Grundrechte, für Zensur und als Statisterie für politische Inszenierungen, dafür sind die Menschen rund um Charlie Hebdo sicher nicht gestanden. Strenggenommen erfolgte

nach Verletzung und Tötung der Opfer damit ihre zweite - grundrechtliche - Verletzung.

Sie werden als Schachfiguren von ahnungs- und orientierungslosen Sicherheitspolitikern und Paranoikern missbraucht. Die Opfer müssen als Faustpfand für neue Polizeirechte, gepanzerte Hubschrauber, neue Vorratsdatenspeicherung, Fluggastdatenerfassung, neue Register und Listen, neue Ghettoisierungsgesetze (vulgo Islamgesetz), Religionsausübung unter staatlicher Kontrolle, weitere Polizeibefugnisse herhalten. Österreich leistet sich hunderte Millionen für eine Sicherheitshochrüstung und nimmt dabei sogar unsinnige Doppelgleisigkeiten zwischen Innenministerium und Verteidigungsministerium in Kauf.

Die Reaktionen der Politik sind faktenfrei, bereiten aber progrommartigen Grundstimmungen den Boden. Bartträger werden bespuckt, Kopftuchträgerinnen beschimpft, Schwarze vor die U-Bahn gestoßen. Nein, wir sind nicht im Jahr 1938, sondern 2015. „Kauft nicht beim Islamisten“, dieser Aufruf fehlt (noch), aber ist „Österreicher zuerst“ soviel besser?

Die drei Attentäter sind tot, doch zahllose Unzufriedene und durchgeknallte Amokläufer werden erstaunt feststellen: So einfach ist es ganze Volkswirtschaften in Chaos und Desorientierung zu stürzen, Staaten dazu zu bringen, Grund- und Verfassungsrechte aufzugeben? Der ideale Nährboden für Nachahmungstäter. [Während diese Analyse verfasst wurde gewinnt die Einschätzung durch den Amoklauf in Kopenhagen grausame Realität.]

Auch das sind leider die Fakten:

Die Mörder haben - mit einem Minimum an Aufwand - alle ihre operativen, taktischen und strategischen Ziele erreicht.

Operativ - die verhassten Kritiker sind ermordet, dazu noch Menschen, deren einziger Fehler war, zur falschen Zeit am falschen Ort gewesen zu sein.

Taktisch - selbst in einem hochgerüsteten Land, mit erfahrenen Polizei- und Anti-Terroreinheiten, weitreichenden Überwachungsbefugnissen können Menschen aus Rand- und Unterschichten erfolgreich Anschläge planen und ausführen. Der Staat kann sich hochrüsten so viel er will, wir können jederzeit zuschlagen, ist die zynische Botschaft.

Strategisch - Aus einer Debatte über sinnvolle Sicherheitsstrategien, sinnvolle Integration und dem nachhaltigen Zusammenleben unterschiedlicher Gruppen wird eine Debatte über Islam, Islamismus und Islamisten. Randgruppen erhalten die Botschaft, sie seien noch weniger erwünscht als bisher. Das Grundrecht auf ein menschenwürdiges Leben, auf soziale Anerkennung, auf Arbeit, Gesundheit und Familienleben bleibt auf der Strecke. Seht, so das strategische Kalkül der Täter, die Grundwerte dieser Gesellschaft werden jederzeit über Bord geworfen, sobald sie sich nur ein bisschen bedroht fühlt.

Wann wird EU-Europa erkennen, dass der von Snowdown aufgedeckte NSA-Skandal nicht ein Überwachungsskandal eines allmächtigen US-Geheimdienstes ist, sondern der Offenbarungseid einer orientierungslosen Loosertruppe, die es mit Milliardenaufwand nicht schaffte die eigenen Daten unter Kontrolle zu halten und der Veröffentlichung durch einen - laut NSA - untergeordneten externen Mitarbeiter (Snowdown) hilflos zusehen musste?

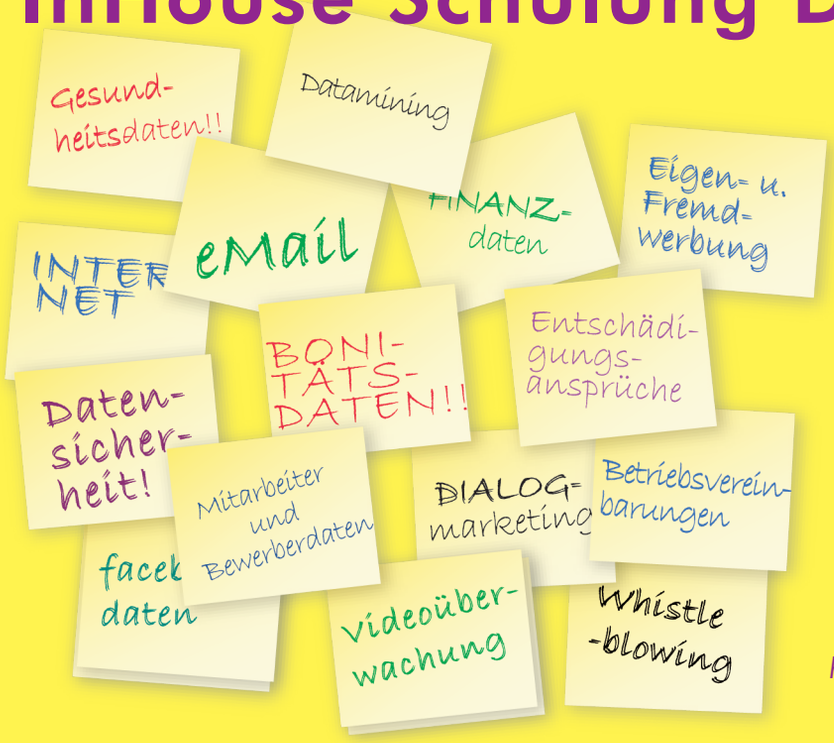
Impressum:

ARGE DATEN - Österr. Gesellschaft für Datenschutz
A-1160 Wien, Redtenbacherg. 20

Fon +43/676/9107032,
Fax +43/1/5320974
www.argedaten.at ,
info@argedaten.at
ZVR 774004629, DVR 0530794

Grundlegende Richtung:
Der Verein bezweckt die Erforschung von Wechselwirkungen zwischen EDV-Einsatz, Informationsrecht, Datenschutz und Gesellschaft (Auszug aus den Statuten §2 Abs.1).
Vorstand: Michael Krenn, Erwin Sulzgruber, Hans Zeger
Grafik: Charlotte Schönherr
Fotos: @ e-commerce monitoring GmbH, Sabine Meyer, Andreas Köckeritz, pixelio.de

InHouse Schulung Datenschutz



Nutzen Sie die Vorteile einer InHouseschulung!

- ✓ *Datenschutz kommt zu Ihnen*
- ✓ *Modulares Konzept*
- ✓ *Unlimitierte Teilnehmerzahl*
- ✓ *Wir beantworten Ihre individuellen Datenschutzfragen*

Ihr individuelles Angebot:
info@e-monitoring.at
fon: +43 1 532 09 44
fax: +43 1 532 09 74
http://seminar.argedaten.at/inhouse

InHouse Schulung Datenschutz die Module

InHouse-Schulung A: DATENSCHUTZ BASIC
Behandelt werden die Grundbegriffe des Datenschutzes. Das Modul bietet allen Mitarbeitern einen ersten Einstieg in die Datenschutzmaterie. Ideal auch zur Datenschutz-Sensibilisierung für alle Mitarbeiter. (1,5 Stunden Vortrag) - Kosten 800,- (inkl. USt. 960,-) + Reiseaufwand*

InHouse-Schulung B: DATENSCHUTZ OVERVIEW
Neben den Grundbegriffen können weitere Datenschutzthemen vertiefend behandelt werden. Entscheiden Sie selbst und wählen Sie zwei Schwerpunkte aus der nebenstehenden Liste aus. Dauer: halbtags (3 Stunden Vortrag + 1 Kaffeepause) - Kosten 1.300,- (inkl. USt. 1.560,-) + Reiseaufwand*

InHouse-Schulung C: DATENSCHUTZ ENHANCED
Nach einer fundierten Einführung wird gezielt auf die spezifischen Probleme Ihrer Organisation eingegangen. Sei es im Umgang mit Kundendaten, Gesundheitsdaten, Bonitätsdaten oder Finanzdaten, im Personalwesen oder bei Data-Mining. Wählen Sie vier Schwerpunktthemen aus der untenstehenden Liste aus. Dauer: ganztags (6 Stunden Vortrag + Mittagspause und 2 Kaffeepausen) - Kosten 2.100,- (inkl. USt. 2.520,-) + Reiseaufwand *

Themenschwerpunkte

- ☐ Überblick allgemein
- ☐ Registrierung von Datenverarbeitungen
- ☐ Auskunfts- und Informationsrechte
- ☐ Internationaler Datenverkehr
- ☐ Videoüberwachung
- ☐ Betriebsvereinbarung Datenschutz
- ☐ Internet/eMail und Datenschutz
- ☐ Datensicherheit
- ☐ Telekommunikation und Datenschutz
- ☐ Datenschutz bei Gesundheitsdaten
- ☐ Mitarbeiter- und Bewerberdaten
- ☐ Whistleblowing
- ☐ eigene Schwerpunkte

☐ Ja, Inhouse Schulung ist für uns ein Thema ☐ kontaktieren Sie uns ☐ schicken Sie uns ein Angebot

<Unternehmen/Organisation> <Postleitzahl/Ort/Anschrift>

<Ansprechpartner/Funktion/Abteilung> <Telefon/Fax/Mailadresse>

<Ort/Datum> <Unterschrift>

* Der Reiseaufwand wird individuell kalkuliert und liegt zwischen 400,- und 800,- Euro. Innerhalb Wiens wird pauschaliert EUR 60,- verrechnet.