ARGE DATEN

DB RECHT 11229 / STELL / Unser Zeichen: eu-stellungnahme-komplett.doc

per FAX: -

An die
European Commission - DG Justice

Rue de la Loi 200 (LX 46 - 01/130)
B-1049 BRÜSSEL

Wien, 13. Januar 2011

Betreff: Konsultation Gesamtkonzept Datenschutz EU

Sehr geehrte Damen und Herren!

Beiliegend finden Sie unsere Stellungnahme zur "MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN - Gesamtkonzept für den Datenschutz in der Europäischen Union" vom 4.11.2010 (KOM(2010) 609 endgültig)

Unsere Identifikationsnummer im Register of interest representatives:
88305294967-50

Sie werden ersucht den Eingang der Stellungnahme zu bestätigen.

Für allfällige Rückfragen stehe ich gern zur Verfügung.

Mit vorzüglicher Hochachtung

Dr. Hans G. Zeger, Obmann

Alle Stellungnahmen werden unter ftp://ftp.freenet.at/ veröffentlicht.

ARGE DATEN - Privacy Austria *A-1160 Wien, Redtenbacherg. 20* *☎ +43/676/9107032, Fax +43/1/4803209*
www.argedaten.at *DVR 0530794* *info@argedaten.at* *Gerichtsstand Wien*
ZVR 774004629 *UID ATU 56627966* *PSK 7.214.741 (BLZ 60000, IBAN: AT15 6000 0000 0721 4741, BIC: OPSKATWW)*

Stellungnahme der ARGE DATEN zum "Gesamtkonzept für den Datenschutz in der Europäischen Union"

Dokument: KOM(2010) 609 endgültig vom 4.11.2010
Identifikationsnummer der ARGE DATEN im Register of interest representatives: 88305294967-50

Inhalt

Vorbemerkung

Die ARGE DATEN informiert und berät in Österreich seit mehr als 20 Jahren Privatpersonen, Unternehmen, öffentliche Einrichtungen und die Medien über Entwicklungen des Datenschutzes, des Schutzes der Privatsphäre und des Schutzes der Grundrechte.

Als Nichtregierungsorganisation (NGO) gelang es uns auf Grund zahlreicher Initiativen und Interventionen die Anliegen des Schutzes persönlicher Daten in zahlreichen Projekten, Gesetzesvorhaben und in der Praxis bei Behörden und Unternehmen besser zu verankern.

Auf Grund unserer Initiative kam es auch zu einer Prüfung der Unabhängikeit der österreichsichen Datenschutz-Aufsichtsbehörde durch die Europäische Kommission (Verfahren läuft).

Wesentliche Leitlinie unserer Tätigkeit ist die Integration und Umsetzung nützlicher Informationstechniken und Informationsdienste in grundrechtskonformer Weise. In diesem Sinn begrüßt die ARGE DATEN grundsätzlich den technischen Fortschritt, der insbesondere durch neue Onlinedienste, neue elektronische Kommunikationsmedien, neue Vernetzungen und neue, meist international organisierte Servicedienste möglich ist.

Die ARGE DATEN verkennt jedoch nicht die Notwendigkeit, dass parallel zum technischen Fortschritt auch die Grundrechte einer ständigen Anpassung und zeitgemäßen Interpretation bedürfen. In diesem Sinn wird die Initiative der Europäischen Kommission für den Bereich Datenschutz eine Gesamtkonzeption zu entwickeln ausdrücklich begrüßt.

Grundsätzliche Feststellungen

Neue Grundrechte

Informationstechnologien erfordern eine Neuinterpretation der Grundrechte. Dies liegt im großteils virtuellen Charakter zahlreicher Informationsdienste, bei denen Grundrechte, die auf bestimmte physische Rechte abzielen (etwa Reisefreiheit, Unversehrtheit der Wohung, Achtung des Familienlebens, ...) nicht oder nur bedingt anwendbar sind.

Insbesondere wird auf das *"Recht auf informationelle Selbstbestimmung"* verwiesen. Jeder Betroffene sollte Anspruch haben vollständig über seine Daten, aber auch die tatsächlich durchgeführten oder konkret beabsichtigten Auswertungen und Interpretationen dieser Daten umfassend informiert zu werden. Dies betrifft ganz besonders Scoring- und Profiling-Dienste, bei denen vielfach aus scheinbar belanglosen oder wenig schützenswerten Einzeldaten weitreichende soziographische Schlüsse gezogen werden und unmittelbar Auswirkung auf die Bonität, die Kreditwürdigkeit, den sozialen Status, seine gesundheitliche Einschätzung oder die Zuverlässigkeit des Betroffenen gezogen werden.

Das "Recht auf informationelle Selbstbestimmung" sollte daher verstärkt und erweitert berücksichtigt werden und jedenfalls Informationsrechte zu verwendeten Scoring- und Profilingverfahren enthalten, unabhängig davon ob sie zur automatisierten oder nicht-automatisierten Entscheidungfindung herangezogen werden. In diesem Zusammenhang sind die Mechanismen zur "informierten Zustimmung", etwa bei der Datenerhebung im Gesundheitsbereich (Stichwort: Genanalyse) zu verbessern.

Als weiteres neu zu adaptierendes Grundrecht sollte die "Unversehrtheit der informationellen Infrastruktur" jedes Betroffenen besser verankert werden. Informationssysteme wie Smartphones, Notebooks, Computer sind nicht mit anderen technischen Konsum- und Haushaltsgeräten, die bloß technische Dienste erledigen, vergleichbar. Sie stellen vielmehr eine Verlängerung (Erweiterung) der persönlichen Privatsphäre dar. Viele Menschen vertrauen diesen Systemen höchst private Gedanken und Ideen an und sie müssen die Sicherheit haben, dass darauf nicht unberechtigt und sanktionslos zugegriffen werden darf.

Zahlreiche Geräte sammeln allein aus der Tatsache, dass sie mit dem Betroffenen mitgeführt werden zahllose persönliche Daten (Stichwort: Geodaten), die auch missbräuchlich verknüpfbar und verwendbar sind.

Insbesondere in Hinblick auf die wachsende Bedeutung des "Internets der Dinge" (KFZ-Technik, Smart-Metering, "Intelligentes" Wohnen, "Intelligente" Kleidung), also der Tatsache

dass immer mehr Geräte über Funkschnittstellen autonom kommunizieren und Daten austauschen, erscheint eine proaktive Regelung dieses Bereichs von großer Bedeutung.

Der Grundsatz der "Unversehrtheit der informationellen Infrastruktur", wie ihn auch das Bundesverfassungsgericht in Deutschland 2008 festhielt, erscheint in der derzeitigen Mitteilung noch nicht ausreichend gewürdigt.

Neudefinition von Personenbezug

Grundsätzlich verwendet die bestehende Richtlinie einen umfassenden Ansatz zur Beschreibung personenbezogener Daten. Als personenbezogen gelten "alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann" (Art. 2 lit a RL 95/46/EG).

Dieser Ansatz konnte 1995 als sehr innovativ angesehen werden und deckte zahlreiche neue Problemstellungen und Entwicklungen ab (Stichworte: Videoaufzeichnungen, biometrische Daten, Biodatenbanken, ...).

Nicht mehr ausreichend abgedeckt werden jedoch neue Entwicklungen bei Online-Diensten, insbesondere im Zusammenhang mit Suchmaschinen, Onlinemarketing, wie behavioral und targteing Marketing, Smartphones usw.

Der bestehende Begriff "personenbezogene Daten" geht direkt oder indirekt von einer fromalen Identifikation mittels Name, Geburtsdatum, Wohnadresse und behördlichen Identifikationsdaten (Personalnummer, Sozialversicherungsnummer, Nummer eines amtlichen Reise- oder Personaldokuments) aus.

Im Zusammenhang mit den neuen Diensten werden jedoch regelmäßig "nur" Programme (Programminstallationen) oder Geräte identifiziert und Daten zu diesem Gerät gesammelt und ausgewertet. Da jedoch die Mehrzahl der Informationssysteme, insbesondere Smartphones, Notebooks, aber auch Arbeitsplatzcomputer regelmäßig nur von ein und derselben Person benutzt wird, ist die Identifikation eines Gerätes de facto die Identifikation eines Benutzers. Geräte, Gerätekennungen und Programmkennungen erfüllen bei Online-Diensten dieselbe Funktion wie Personalausweise im klassischen Leben, sie sollten daher als Identifikationskennzeichen gleichgestellt werden.

Die bei den Onlinediensten verwendeten Identifikationskriterien, wie Cookies, individuelle URLs (Webadressen), Gerätesignaturen, Maschinenadressen (MAC-Adresse, IP-Adresse, IMSI- oder IMEI-Adresse bei Mobiltelefonen) zur Identifikation ein und desselben Gerätes sind zumindest genauso effektiv, wie Personalnummern. Im Unterschied zu amtlichen Identifikationssystemen existieren zwar keine Verknüpfungen zu bestimmten Namen, aber es lassen sich trotzdem präzise Aussagen über das Verhalten des jeweiligen Gerätebenutzers machen. Der Benutzer kann gezielt mit bestimmten Informationen (etwa Onlinewerbung) versorgt werden bzw. können Benutzern mit bestimmten Profilen bestimmte Informationen vorenthalten oder vorgefiltert werden.

Unter anderem ist bekannt, dass Suchmaschinen Trefferreihungen vom Standort des Anfragers abhängig machen oder Anbieter von Online-Mailboxen Werbung und sonstige Informationen in Abhängigkeit zum Mailinhalt einblenden.

Damit wird ein Personenbezug hergestellt, der den bisherigen personenbezogenen Diensten gleichwertig ist, aber derzeit nicht geregelt ist. Man kann von einer *funktionalen Identifikation* einer Person sprechen, die jahrelang ohne formale Zuordnung zu einem bestimmten Namen oder zu einer amtlichen Personalnummer auskommt. Reagiert jedoch diese Person auf bestimmte Angebote, dann kann ihr gesamtes bisheriges Surf-, Such- oder eMail-Verhalten aufgerollt werden.

Es ist dringend notwendig, Betroffenen im Zusammenhang mit funktionaler Identifikation den bisherigen Auskunfts- und Informationsrechten gleichwertige Rechte einzuräumen.

Sobald Datenverarbeiter individualisierte Aufzeichnungen führen, also individualisiert Suchabfragen bestimmten Identifikationskriterien zuordnen oder (Geo-)daten der Smartphonebenutzer bestimmten Smartphoneadressen zuordnen, soll es Benutzern möglich sein durch Bekanntgabe ihrer gerätespezifischen Identifikationskriterien (siehe oben) Auskunft über die verwendeten Daten zu erhalten und dieselben Löschungs- und Richtigstellungsrechte zu haben, wie bei sonstigen bestimmten Personeninformationen.

Die Privilegierung derartiger Daten als "indirekt personenbezogene Daten", wie dies bei manchen EU-Staaten der Fall ist (etwa Österreich) sollte jedenfalls ausgeschlossen werden.

Technikneutralität

Grundsätzlich wird begrüßt, dass die Mitteilung dem Grundsatz der Technikneutralität verpflichtet bleibt. Realistischerweise ist jedoch anzumerken, dass eine völlige Technikneutralität nicht möglich ist oder bloß zu sehr abstrakten und damit unverbindlichen Absichtserklärungen führt.

Es wird angeregt weitgehend technikneutral, im Sinn des Verzichts auf einen Bezug auf bestimmte technische Standards, Protokolle und IT-Systeme zu formulieren. Umgekehrt sollte jedoch nicht dienstneutral vorgegangen werden. Übertragungsmethoden per Funk (statt drahtgebunde Übertragung) oder Online-Dienste statt Offline-Dienste usw. enthalten eben neue spezifsiche Risken, die nur durch Bezug auf den konkreten Dienst dargestellt und geregelt werden können.

In diesem Sinn sollte etwa auf die Verwendung von Begriffen wie Internet, RFID, GSM usw. verzichtet werden, dafür sollten die dahinterliegenden Dienste benannt werden (also Online-Dienst statt Internet-Dienst, Funkübertragung statt RFID, ...).

Zentrale Anliegen

Besserer Evaluationsmechanismus für die innerstaatliche Umsetzung

Eine Neuorganisation des Datenschutzes auf EU-Ebene sollte bessere Umsetzungskontrollen als bisher enthalten. Die Erfahrungen der letzten 15 Jahre zeigten, dass eher Probleme in der innerstaatlichen Umsetzung (etwa bei der Ausstattung der Aufsichtsbehörden oder bei den Sanktionen) bestanden, als eigentlich Mängel in der Richtlinie.

Dies könnte einerseits durch klarere Vorgaben erfolgen, andererseits auch durch einen besseren institutionalisierten Konsultationsmechanismus der Mitgliedsstaaten untereinander. Aufgabenbereich und Tätigkeit der Art. 29 - Gruppe ist als Schritt in die richtige Richtung anzusehen, sollte jedoch ausgeweitet werden.

Stärker als bisher sollte auf ein gleichwertiges Schutz- und Sanktionsniveau für alle EU-Staaten geachtet werden.

Bessere EU-weite Standardisierung und Integration

Eine wesentliche Erfahrung der letzten 15 Jahre war die stark fortschreitende Integration wirtschaftlicher Tätigkeit zwischen den EU-Staaten. Es ist für zahllose Unternehmen selbstverständlich geworden in mehreren EU-Staaten Tochterunternehmen oder Niederlassungen zu betreiben.

Unterschiedliche Registrierungs- und Aufsichtsverfahren im Bereich Datenschutz führen jedoch zu unnötiger Bürokratie und Doppelgleisigkeiten.

Für bestimmte Bereiche, wie die Registrierung von Datenanwendungen, für die Genehmigung im internationalen Datenverkehr sollten einheitliche Formulare und Abläufe verbindlich für alle EU-Staaten festgehalten werden und Genehmigungen eines Staates auch für dieselben Datenverarbeitungen in Niederlassungen anderer EU-Staaten gelten.

Zur Sicherung der Transparenz für die Betroffenen sollte ein EU-weites Register eingerichtet werden, das alle registrierten Datenanwendungen umfasst bzw. die verantwortlichen Datenschutzbeauftragten der Organisationen auflistet.

Weiters sollte es für international agierende Unternehmen mit Niederlassungen in mehreren EU-Staaten für alle seine Niederlassungen in allen EU-Staaten möglich sein zwischen der Registrierung bei einer Aufsichtsstelle oder der Nominierung eines betrieblichen Datenschutzbeauftragten zu wählen.

Jedenfalls sollte in jedem EU-Land die Möglichkeit für Datenverarbeiter vorgesehen werden, statt ihre Datenverarbeitungen direkt einer zentralen Aufsichts- und Registrierungsstelle zu unterstellen einen verantwortlichen betrieblichen Datenschutzbeauftragten zu nominieren. Dies hätte gerade für Eu-weit agierende

Unternehmen enorme Einsparungspotentiale und Synergiewirkungen und wäre - ohne Grundrechtsverlust - eine Stärkung der Binnenmarktkomponente

In der gegenwärtigen Situation ergeben sich für viele Unternehmen Doppelgleisigkeiten durch unterschiedliche Registrierungsverfahren in einzelnen EU-Ländern plus erforderlichen Datenschutzbeauftragen in anderen EU-Ländern. Eine unnötige Bürokratisierung, die keinerlei Vorteil für Betroffene hat.

Bessere Durchsetzbarkeit von Betroffenenrechten

Insbesondere der vermehrte Einsatz von Onlinediensten erfordert eine Neudefinition des Niederlassungsprinzips.

Die bisherige Richtlinie ging im wesentlichen von der Ortsidentität von Datenverarbeiter und Betroffenen aus. Beide befinden sich an demselben Ort, einem Amt, einer Bankfiliale, einer Arztpraxis usw. Zur Klarstellung des geltenden Rechts machte es Sinn diesen Ort, der der Standort des Verarbeiters war, zum relevanten Rechtsstandort zu erklären. Es wäre einem Bankangestellten nicht zumutbar gewesen einen Kunden abhängig von seiner Herkunft nach unterschiedlichen Datenschutzregeln zu behandeln.

Dieser vernünftige Grundsatz wird jedoch bei Onlinediensten zu einem Problem. Hier kann der Betriebsort beliebig verlegt werden, die datenschutzrelevanten Aktivitäten (etwa Datenerfassung, Datenabruf, Datenanzeige) finden an beliebigen anderen Orten oder am Endgerät des Betroffenen statt.

Für Onlineangebote sollte vom -willkürlich einsetzbaren - Niederlassungsprinzip abgegangen werden und stattdessen der Wohnsitz des Betroffenen als Rechtsgrundlage für die Durchsetzung der Datenschutzrechte herangezogen werden. Dieses Prinzip findet bei der Verfolgung von unerlaubter Werbung (etwa eMail-Spam) schon jetzt seine Anwendung, hier ist der Tatbegehungsort nicht der oft nicht lokalisierbare Mailserver, der den Spam versendet, sondern der Ort, an dem das Spam-Mail ankommt.

Dies hätte eine wesentlich verbesserte Rechtsstellung der Betroffenen zur Folge, für die Datenverarbeiter wäre ein möglicher Zusatzaufwand relativ gering, wenn die vorher angeregten Harmonisierungsschritte konsequent verfolgt werden.

Im Zusammenhang mit Onlinediensten die über überhaupt keine Niederlassung innerhalb der EU verfügen sollten verstärkt Kooperationsabkommen zwischen EU-Kommission und den jeweiligen Drittstaaten, in denen der Anbieter seinen Sitz hat, den Schutz der EU-Bürger sicher stellen.

Weiters sollte die Kooperation der Aufsichtsstellen enger gestaltet werden. Es sollte für Betroffene möglich sein und die Aufsichtsstellen verpflichten, Beschwerden, Anfragen usw. zu jedem EU-Datenverarbeiter bei jeder EU-Aufsichtsstelle einzubringen. Diese hätte sie dann allein oder in Kooperation mit der jeweiligen nationalen Aufsichtsstelle zu behandeln. Sinnvoll wäre eine Konstruktion vergleichbar dem Informationsrecht aus dem Schengener Informationssystem (SIS), das der Betroffene gegenüber jedem SIS-Teilnehmer in Anspruch

nehmen kann und in Folge bei der zugeordneten Aufsichtsbehörde Beschwerde erheben kann (womit de facto eine Wahlfreiheit in der Beschwerdestelle gegeben ist).

Anmerkungen zur Mitteilung im Detail

Hinweis

Positionen und Schlussfolgerungen der Kommission, die nicht kommentiert werden, werden uneingeschränkt begrüßt.

Generelle Anmerkungen

Uneingeschränkt zuzustimmen ist der Kommission hinsichtlich der Diagnose zunehmender Gefahren für die Privatsphäre durch die immer weiter ausgreifende Nutzung von Online-basierten Technologien (Stichworte: „Soziale Netzwerke“, „Cloud Computing“ etc.) oder Anwendungen, die sich auf Mobilfunk jeweils in Verbindung mit Verfahren der automatisierten elektronischen Standortbestimmung oder RFID-Technologien stützen (Bsp: elektronische Mautsysteme, elektronische Tickets in öffentlichen Verkehrsmitteln etc.).

Die konkrete *Beantwortung* der *Frage,* wie die *Auswirkungen* der genannten Technologien datenschutzrechtlich *beherrschbar* gemacht werden können, ist derzeit jedoch noch zu vage.
Es werden einige wichtige Aspekte angesprochen (etwa: verständliche Informationen der Betroffenen, Kontrolle über die „eigenen Daten“ im Rahmen von sozialen Online-Netzwerken, Präzisierung der Regelungen über die „Einwilligung“ oder „anwenderfreundlichere“ Gestaltung der Regelungen über das anwendbare Datenschutzrecht).

Andere praktische Probleme, die sich vor allem im Rahmen von Online-Diensten stellen, bleiben ausgeklammert oder werden nicht ausreichend gewürdigt.

Konkret geht es um den rechtlichen Umgang mit dem Bestreben bestimmter Auftraggeber (Suchmaschinenbetreiber), *umfassende Datensammlungen* über das *Nutzungsverhalten* Betroffener anzulegen und diese anhand bestimmter Kriterien *auszuwerten* („Datamining“, „Profilbildung“ bzw. „Profiling“) und ggf. mit Daten aus *weiteren Anwendungen zu verknüpfen*.

Ein weiters von der Datenschutzrichtlinie nicht gelöstes Problem ist die Frage der *Transparenz* grenzüberschreitender Informationsverbundsysteme. Bei solchen Datenanwendungen mit mehreren datenschutzrechtlichen Auftraggebern mit Sitz in verschiedenen Mitgliedstaaten stellt sich konkret die Frage nach einem einheitlichen Registrierungsverfahren. Der derzeitige Rahmen der Richtlinie (Art. 18 ff) geht erkennbar von einer rein lokalen Betrachtungsweise aus.

Die Betonung des Prinzips der *Datensparsamkeit* verdient uneingeschränkte Unterstützung. Zugleich darf kritisch angemerkt werden, dass gerade einzelne für das Jahr 2011 in Aussicht genommene Gesetzesvorschläge bzw. Vorarbeiten der Kommission diesem Gebot

diametral entgegenlaufen. Zu nennen sind hier v.a. der angekündigte Legislativvorschlag zur Einrichtung des automatisierten Einreise-/Ausreisesystems, die Mitteilung über ein ESTA-System der EU, die angedachte Richtlinie über die Verwendung von Fluggastdatensätzen zu Strafverfolgungszwecken (Europäische PNR) oder das Europäische Programm zum Aufspüren der Finanzierung des Terrorismus. Nicht zu reden von der bereits in Kraft befindlichen Richtlinie 2006/24/EG (Vorratsspeicherung von Daten).

Mit Vorbehalt zu sehen sind auch die Ausführungen der Kommission zur *„Binnenmarktdimension“* des Datenschutzes. Zwar trifft es zu, dass ein zentrales Motiv hinter der Erlassung der Datenschutzrichtlinie in der Erreichung eines *„freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten“* war. Zu betonen ist allerdings, dass dieser Aspekt mittlerweile durch das Inkrafttreten der Grundrechtecharta der EU quasi überlagert bzw. ergänzt wurde. Das Ziel des Abbaus von Verwaltungsaufwand beim grenzüberschreitenden Datenverkehr ist insofern kein absolutes Motiv mehr, sondern bedarf nach dem Vertrag von Lissabon einer grundrechtskonformen Deutung.

Mit Nachdruck zu begrüßen ist die von der Kommission angestrebte *Einbeziehung* der Bereiche der *polizeilichen und justiziellen Zusammenarbeit* in Strafsachen *in den Anwendungsbereich* der *allgemeinen* Datenschutzrichtlinie. Tatsächlich kann der bestehende Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, nur als erster Schritt gesehen werden, dessen *Defizite* die Kommission *zutreffend anführt*.

Zu begrüßen ist die kritische Auseinandersetzung mit der Frage des *„Datenexports“ in Drittstaaten*. Tatsächlich fehlt es im Bereich der früheren „dritten Säule“ völlig an entsprechenden Vorgaben, was zu einer völlig uneinheitlichen Praxis im Vergleich der Mitgliedstaaten führt. Auch im Anwendungsbereich der Datenschutzrichtlinie haben die bestehenden Vorgaben – wie die Kommission zutreffend feststellt - zu keinen befriedigenden Ergebnissen geführt. Auch dort, wo ein gemeinsames Vorgehen der EU bzw. ihrer Mitgliedstaaten Platz greift, gelingt es bis dato allerdings nicht, eine nachdrückliche, glaubwürdige und vor allem wirksame Datenschutzpolitik gegenüber Drittstaaten zu betreiben (Stichwort: SWIFT-Abkommen EU-USA).

Zu Abschnitt 2.1. Stärkung der Rechte des Einzelnen

2.1.1. Angemessener Schutz des Einzelnen in allen Situationen

> Die Kommission wird prüfen, **wie eine kohärente Anwendung der Datenschutzvorschriften sichergestellt werden kann unter Berücksichtigung der Auswirkungen neuer Technologien auf die Rechte und Freiheiten von Personen mit dem Ziel, den freien Verkehr personenbezogener Daten im Binnenmarkt zu gewährleisten.**

Vordringlicher Handlungsbedarf besteht im Bereich der *Internetnutzung* durch User. Daraus ergeben sich unter anderem folgende Regelungsanforderungen:

- Bestimmungen über die *Funktionalitäten von Suchmaschinen:*Nutzern sollte zwingend die Möglichkeit eröffnet werden, eine Variante zu wählen, bei der eine Speicherung des

Suchverhaltens nach Abschluss einer Suche bzw. „Sitzung“ durch den Suchmaschinenanbieter unterbleibt.
- Bestimmungen über die Zulässigkeit bzw. Unzulässigkeit der *„Profilbildung“* (Erstellung von Nutzerprofilen, Persönlichkeitsprofilen) mittels im Internet verfügbarer Daten
- Bestimmungen über die *spezifischen Informationspflichten* von Online-Diensteanbietern gegenüber Nutzern
- Grundlegende Bestimmungen über die *Rechtsstellung von Nutzern* von sozialen Online-Netzwerken gegenüber den Anbietern einschlägiger Plattformen. Diese sollten insbesondere das Recht der Nutzer auf jederzeitige Änderung oder vollständige Löschung ihrer Daten umfassen. Eine unbeschränkte Nutzung solcher Daten für eigene Zwecke des Diensteanbieters oder für Zwecke Dritter sollte auch durch die Einwilligung des Nutzers nicht zulässig werden.
- Es sollte ein Recht auf *grundsätzlich anonyme Nutzung* von kostenlosen *Online-Informationsangeboten* verankert werden. Dies erscheint insbesondere auch mit Blick auf das Grundrecht auf Freiheit der Meinungsäußerung und Informationsfreiheit gemäß Art. 11 der Grundrechtecharta geboten. Auch in Bezug auf kostenpflichtige Informationsangebote sollte der Grundsatz gelten, dass im Wege alternativer Zahlungsmittel (Stichwort: Guthabenskarten bzw. „Prepaid“-Karten) eine anonyme Nutzungsvariante so weit wie möglich gewährleistet wird.
- „Anonymisierungs-Server“: Initiativen der Zivilgesellschaft, welche eine anonyme Nutzung des Internets durch Bereitstellung technischer Mittel ermöglichen, sollten gefördert werden.

Das Prinzip der anonymen Nutzung von Online-Dienstleistungen soll sinngemäß auch für andere Datenverarbeitungsbereiche angewandt werden. So ist davon auszugehen, dass sich aus dem Grundrecht auf Privatsphäre insbesondere das Recht ergibt, öffentliche Straßenverkehrsinfrastruktur zu nutzen, ohne dabei von staatlicher oder privater Seite einer systematischen Beobachtung ausgesetzt sein zu müssen:
- Anbieter öffentlicher Verkehrsdienstleistungen sollten stets und diskriminierungsfrei eine Nutzungsvariante anbieten, die ohne die Erhebung personenbezogener Daten das Auslangen findet (Barzahlung, Bezahlung mittels nicht personengebundener elektronischer Medien, elektronischer Geldbörsen).
- Es sollte im Bereich des Straßenverkehrs festgelegt werden, dass allfällige Nutzungsgebühren (Maut) stets auch in nicht personenbezogener Form entrichtet werden können.
- Technische Einrichtungen zur Verkehrsüberwachung oder zur Erfassung der Verkehrsfrequenz, die auf bildgebenden Verfahren basieren, müssen so konzipiert sein, dass eine personenbezogene Erfassung Betroffener tunlichst vermieden wird.

Besonderes Augenmerk ist auf den Umgang mit „Standortdaten“ bzw. „Geodaten“ zu richten. Um die Privatsphäre der Betroffenen nicht über den Umweg der Generierung bzw. Speicherung und Weiterverarbeitung solcher Daten zu gefährden, sollten insbesondere nachstehende Grundsätze verankert werden:
- Die über das technisch erforderliche Ausmaß hinausgehende Verarbeitung und Speicherung von personenbezogenen Standortdaten muss grundsätzlich unzulässig sein.
- Besitzer von Immobilien (ausgenommen historische bzw. staatliche Immobilien) sollten das Recht erhalten, der fotographischen Reproduktion ihrer Immobilie im Rahmen von

Geodaten-basierten Online-Angeboten, die eine Identifizierung des Besitzers /Nutzers der Immobilie ermöglichen, zu widersprechen. Auf ein solches Widerspruchsrecht müssen die Betroffenen in geeigneter Form hingewiesen werden (Anzeigen in Medien etc.). Die Ausübung eines solchen Widerspruchsrechts darf nicht zeitlich beschränkt werden, sondern muss auch nachträglich jederzeit möglich sein.
- Im Falle der systematischen automatisierten Erfassung von Örtlichkeiten bzw. Immobilien zwecks Zugänglichmachung im Rahmen eines Online-Dienstes müssen auf den Aufnahmen erkennbare Personen vollständig und zuverlässig unkenntlich gemacht werden. Dies muss auch für Kfz-Kennzeichen uä. identifizierende Merkmale gelten. Das unkenntlich Machen hat zeitnah und jedenfalls in dem Land zu erfolgen, in dem die Aufnahmen und Aufzeichnungen erfolgten. Keinesfalls dürfen Daten aus diesen Diensten personenbezogen (individualisiert) in ein Drittland verbracht werden.

Als ein weiteres Problemfeld stellt sich die Digitalisierung bzw. „Computerisierung" der Kfz-Branche dar. Moderne Pkws sind mit einer Vielzahl technischer Sensoren ausgestattet, welche während der Nutzung umfassende Daten sammeln. Diese werden anlässlich von Wartungen in Vertragswerkstätten des Herstellers ausgelesen und online an eine zentrale Anwendung übermittelt. Letztere ist solcherart in der Lage, Rückschlüsse auf den Fahrzeugzustand, aber auch auf den Nutzungsmodus (Fahrgewohnheiten) zu ziehen. Den wenigsten Verbrauchern ist dieser Umstand bewusst. Es erscheint angezeigt, auch diesem Feld unter dem Gesichtspunkt der Transparenz bzw. anzustrebenden Selbstbestimmung der Betroffenen entsprechende regulatorische Aufmerksamkeit zu widmen.

Spezifischer Regelungsbedarf besteht schließlich auch in Bezug auf den Einsatz bildgebender Verfahren zu Überwachungszwecken („Videoüberwachung"), sei es durch Private, sei es durch staatliche Stellen.
Als Grundsätze für diesbezügliche spezifische Regelungen sollten insbesondere die Folgenden erwogen werden:
- Höchstpersönliche Lebensbereiche bzw. Situationen, die in direktem Bezug zur höchstpersönlichen Sphäre Betroffener stehen, dürfen grundsätzlich nie Gegenstand einer Überwachung mittels bildgebender Verfahren sein (Bsp: Toiletten und deren Zugänge, Umkleidekabinen, Spitals- und Pflegebetten mit Ausnahme von Intensivstationen etc.).
- Eine permanente Videoüberwachung von Mitarbeitern an ihrem Arbeitsplatz zur Leistungskontrolle muss unzulässig sein.
- Videoüberwachungen im öffentlichen Raum bedürfen einer besonderen Rechtfertigung und müssen einer strengen Verhältnismäßigkeitsprüfung im Einzelfall unterworfen werden.
- Im Falle von Videoaufzeichnungen muss die Speicherdauer auf das unbedingt erforderliche Maß begrenzt werden.
- Durch Videoüberwachungen darf das Prinzip der anonymen Nutzung von öffentlicher Infrastruktur (Stichwort: Barzahlung am Automaten), von Online-Informationsangeboten (Stichwort: Internetcafé) etc. nicht unterlaufen werden.
- Besondere Eingriffe in die Privatsphäre können sich durch den Einsatz von Mini-Drohnen durch Private ergeben, die beispielsweise direkt Bilder auf ein Smartphone übertragen können sowie durch den unkontrollierten Einsatz von Spionagesatelliten (z.B. HIROS-Projekt von Deutschland und USA).

2.1.2. Mehr Transparenz für die von der Verarbeitung Betroffenen

> Die Kommission wird folgende Maßnahmen in Erwägung ziehen:
>
> - Einführung eines allgemeinen **Transparenzgrundsatzes für die Verarbeitung** personenbezogener Daten in der Datenschutzregelung;
>
> - Einführung **besonderer Pflichten** für die Verantwortlichen für die Verarbeitung, was die Art der Informationen und die **Modalitäten** der Bereitstellung dieser Informationen anbelangt, auch in Bezug auf **Kinder**;
>
> - Erstellung eines oder mehrerer **EU-Standardmuster („Datenschutzhinweise")**, die die für die Verarbeitung Verantwortlichen zu verwenden haben.

Auch hier besteht gerade im Online-Bereich ein verstärkter Bedarf zur Verbesserung der Transparenz. Verbindliche Regelungen auf EU-Ebene sind erforderlich uns sollten folgende Aspekte umfassen:

- Einwilligungsklauseln im Online-Bereich dürfen nicht in Allgemeinen Geschäftsbedingungen „versteckt" sein, sondern müssen gesondert und in für den Nutzer leicht erkennbarer und lesbarer Form präsentiert werden.
- Vorformulierte Einwilligungserklärungen im Online-Bereich dürfen nicht als Opt-out-Lösungen, sondern nur als Opt-in-Lösungen konzipiert sein. Dies betrifft insbesondere Voreinstellungen, die die Veröffentlichung oder Weitergabe persönlicher Daten betreffen. Soweit Alternativen sinnvoll sind und angeboten werden, haben die Voreinstellungen immer keine Veröffentlichung oder Weitergabe zu sein.
- Die datenschutzrechtlichen Einwilligungserklärungen müssen von den Erklärungen, mit denen sonstige „Vertragsinhalte" angenommen werden, abgesondert und unabhängig voneinander eingeholt werden.

Die genannten Grundsätze haben auch im Offline-Bereich nicht nur große praktische Relevanz, sondern sind dort gesetzlich vorgeschrieben. Sie sollten insofern auch in der allgemeinen Datenschutzrichtlinie für alle schriftlichen Einwilligungen verankert werden.

> Die Kommission wird
>
> - die Modalitäten für die Einführung einer **allgemeinen Anzeigepflicht für Datenschutzverstöße** in der allgemeinen Datenschutzregelung prüfen, einschließlich der Adressaten solcher Anzeigen und der Umstände, die eine Anzeigepflicht begründen.

Diese Position wird ausdrücklich unterstützt und sollte jedenfalls unabhängig von Schadensbewertungen durch den Datenverarbeiter erfolgen. Diese Anzeige und Informationspflicht dient der Gefahrenabwehr und der erleichterten Durchsetzung von Schadenersatzansprüchen dadurch geschädigter Personen. Darüber hinaus ist auch eine generalpräventive Wirkung zu erwarten, da Veröffentlichungen von Datenschutzverstößen, vergleichbar den Rückrufaktionen bei Produktschäden wettbewerbsnachteile nach sich ziehen können.

2.1.7. Wirksamere Rechtsbehelfe und Sanktionen

> Die Kommission wird
>
> - prüfen, ob die **Befugnis zur Klage bei nationalen Gerichten** auch auf Datenschutzbehörden und Verbände der Zivilgesellschaft sowie andere **Verbände, die die Interessen der von der Verarbeitung Betroffenen vertreten**, ausgedehnt werden kann;
>
> - untersuchen, ob die **bestehenden Sanktionsregelungen verschärft** werden sollten, beispielsweise durch strafrechtliche Sanktionen bei ernsten Datenschutzverletzungen, damit die Sanktionen mehr Wirkung zeigen.

Beide Positionen werden ausdrücklich unterstützt, wobei auch hier eine Vereinheitlichung der Sanktionsregelungen und ein möglichst niederschwelliger Zugang zu Beschwerdemöglichkeiten oberstes Gebot haben sollen.

Zu Abschnitt 2.2. Stärkung der Binnenmarktdimension

2.2.2. Verringerung des Verwaltungsaufwands

> Die Kommission wird verschiedene Möglichkeiten für eine **Vereinfachung und Harmonisierung der derzeitigen Melderegelung** prüfen, darunter die Einführung eines **EU-weit einheitlichen Registrierungsformulars**.

Die Schaffung eines einheitlichen Registrirrungsformulars liegt sowohl im Interesse der Datenverarbeiter, als auch der Betroffenen, ist aber jedenfalls durch eine zentrale Informationsstelle über die tatsächlich durchgeführten Registrierungen zu ergänzen.

2.2.3. Klärung der Bestimmungen über das anwendbare Recht und der Verantwortung der Mitgliedstaaten

> Die Kommission wird prüfen, wie die geltenden **Vorschriften über das anwendbare Recht** sowie die Kriterien zu dessen Bestimmung **geändert und präzisiert** werden können, um für mehr Rechtssicherheit zu sorgen, die Zuständigkeit der Mitgliedstaaten für die Anwendung der Datenschutzvorschriften zu klären und letztlich den von der Verarbeitung Betroffenen in der EU unabhängig vom geografischen Standort des für die Verarbeitung Verantwortlichen stets ein gleiches Schutzniveau zu garantieren.

Insbesondere im Zusammenhang mit Online-Diensten muss sicher gestellt werden, dass durch die Wahl der Niederlassung durch den Dienstbetreiber nicht de facto die Datenschutzrechte der Betroffenen geschmälert werden. Hier sei auf das konkrete Beispiel www.norc.at verwiesen. Hier erfolgen Aufnahmen durch den rumänischen Datenverarbeiter in anderen EU-Staaten, etwa Österreich. Betroffene müssten jedoch Beschwerden an die rumänische Datenschutzbehörde nach rumänischem Recht in rumänischer Sprache einbringen. Das ist für Betroffene aus praktischer Sicht schlicht unzumutbar.

Weiters wurde auch schon beobachtet, dass deutsche und österreichische Online-Datenverarbeiter formal ihren Sitz in die Slowakei verlegen, ihre Dienste aber ausschließlich deutsch für Deutsche und Österreicher anbieten und auch die tatsächliche

technische Verarbeitung in Österreich/Deutschland stattfindet. Betroffene müssten aber nach slowakischem Recht in slowakischer Sprache bei der slowakischen Behörde Beschwerde erheben. Was schon angesichts von Übersetzungsproblemen zu Verzögerungen und damit zu Fristversäumnissen führen kann.

Es wird angeregt, im Rahmen des neuen umfassenden Rechtsrahmens für den Datenschutz die Zuständigkeitsregelungen dahingehend abzuändern, dass bei der Verletzung datenschutzrechtlicher Vorschriften durch ausländische Datenverarbeiter ohne Niederlassung in dem betroffenen Mitgliedstaat generell die inländische Datenschutzbehörde für Beschwerden von im Inland Betroffenen zuständig gemacht wird.

Es sollte jedenfalls der Grundsatz des Konsumentenschutzrechtes gelten, dass Dienste die sich offensichtlich an eine bestimmte Betroffenengruppe wenden (etwa auf Grund der verwendeten Sprache, des Angebots) bzw. Daten dieser Betroffenengruppe systematisch verwenden (etwa durch Datenerhebung vor Ort) auch nach dem nationalen Recht dieser Gruppe behandelt werden.

Zu Abschnitt 2.3. Änderung der Datenschutzvorschriften in den Bereichen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Die Kommission wird

- die **Einbeziehung der Bereiche der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in den Anwendungsbereichs der allgemeinen Datenschutzbestimmungen** prüfen, und zwar auch bei einer rein innerstaatlichen Verarbeitung, gegebenenfalls bei gleichzeitiger Einführung harmonisierter **Einschränkungen** bestimmter Datenschutzrechte von Personen, z. B. hinsichtlich des Zugriffsrechts oder des Transparenzprinzips;

- prüfen, ob die neue allgemeine Datenschutzregelung **besondere, harmonisierte Vorschriften** enthalten sollte, beispielsweise für den Datenschutz bei der Verarbeitung von **Gendaten** zu strafrechtlichen Zwecken, oder unterschiedliche Vorschriften für verschiedene Gruppen von Betroffenen (Zeugen, Verdächtigte usw.) im Bereich der Zusammenarbeit zwischen den Polizeibehörden und der justiziellen Zusammenarbeit in Strafsachen;

- 2011 eine **Konsultation** aller interessierten Kreise durchführen, um ihre Meinung zu den bestehenden Verfahren zur **Änderung des derzeitigen Kontrollsystems im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** einzuholen und so eine wirksame, kohärente Datenschutzkontrolle in den Einrichtungen, Ämtern und Agenturen der EU sicherzustellen;

- prüfen, ob die **in einzelnen Rechtsakten enthaltenen sektorspezifischen EU-Vorschriften für die polizeiliche und justizielle Zusammenarbeit in Strafsachen** langfristig an die neue allgemeine Datenschutzregelung **angepasst** werden sollten.

Begrüßt wird das Ziel, die bestehenden Regelungen für den Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit zu stärken und auf das Schutzniveau der allgemeinen Datenschutzrichtlinie anzuheben. Besonderes Augenmerk ist dabei auf den Zweckbindungsgrundsatz sowie die Wahrung eines angemessenen Schutzniveaus bei

Datentransfers in Drittstaaten zu legen. Mittel- und langfristig setzt die weitere Intensivierung der polizeilichen und justiziellen Zusammenarbeit zwischen den Mitgliedstaaten zwingend die Annäherung auch des materiellen und prozessualen Polizei- und Strafrechts auf hohem Schutzniveau voraus.

Bestehende Instrumente, insbesondere auch bilaterale Amts- und Rechtshilfeabkommen der Mitgliedstaaten untereinander sowie mit Drittstaaten sollten mittelfristig in datenschutzrechtlicher Hinsicht zwingend angepasst werden und der neuen Rechtslage (nach Schaffung des neuen umfassenden Datenschutzinstrumens) gebührend Rechnung tragen. Eine entsprechende regulatorische Vorgabe wäre anzustreben.

Notwendig wäre auch die ausdrückliche Verankerung eines allgemeinen Grundsatzes, wonach auch für Zwecke der polizeilichen und justiziellen Zusammenarbeit verdachtsunabhängige Überwachungsmaßnahmen, die Bevölkerung insgesamt bzw. eine gesamte soziale Gruppe treffen, nie zulässig sein dürfen.

Zu Abschnitt 2.4. Die globale Dimension des Datenschutzes

Zu Abschnitt 2.5. Verstärkter institutioneller Rahmen für eine bessere Durchsetzung der Datenschutzvorschriften

> Die Kommission wird prüfen,
>
> - wie die **Rechtsstellung und die Befugnisse der nationalen Datenschutzbehörden in der neuen Regelung gestärkt, präzisiert und harmonisiert** werden können, darunter auch durch die uneingeschränkte Durchsetzung des Grundsatzes der völligen Unabhängigkeit;
>
> - wie die **Zusammenarbeit und Abstimmung zwischen den Datenschutzbehörden verbessert** werden kann;
>
> - wie eine kohärentere Anwendung der Datenschutzvorschriften der EU im gesamten Binnenmarkt sichergestellt werden kann. Beispielsweise kommen folgende Maßnahmen in Frage: **Stärkung der Rolle der nationalen Datenschutzbeauftragten, bessere Koordinierung ihrer Tätigkeiten über die Datenschutzgruppe (die transparenter werden sollte) und Einführung eines Verfahrens zur Sicherstellung einer einheitlichen Praxis im Binnenmarkt unter der Zuständigkeit der Europäischen Kommission.**

Die Zusammenarbeit der nationalen Datenschutzbehörden muss in Hinblick auf eine Vereinheitlichung von Sanktionen und Auslegung der EU-Vorgaben verbessert werden. Dies erleichtert die Tätigkeit der Datenverarbeiter und erhöht die Rechtssicherheit der Betroffenen.