REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ BKA-825.202/0002-DSR/2011
TELEFON (+43 1) 53115/2527
FAX (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Europäische Kommission
Generaldirektion Justiz und Grundrechte
Referat C3 – Datenschutz
B - 1049 Brüssel

Betrifft: **Konsultationsverfahren betreffend die Mitteilung der Kommission „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vom 4. November 2010 (KOM[2010] 609 endg)**
Stellungnahme des Datenschutzrates

I. Vorbemerkung

Der **Österreichische Datenschutzrat** berät als unabhängiges Beratungsorgan die Bundesregierung in rechtspolitischen Fragen des Datenschutzes. Zur Erfüllung dieser Aufgabe kann der Datenschutzrat Fragen von grundsätzlicher Bedeutung für den Datenschutz in Beratung ziehen und Gutachten zu datenschutzrechtlichen Vorhaben erstellen. Im Rahmen seiner Zuständigkeit für die Wahrung des Datenschutzes hat der Datenschutzrat die Mitteilung der Kommission über ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vom 4. November 2010, einer intensiven Diskussion unterzogen und in seiner 203. Sitzung am 24. Jänner 2011 **einstimmig beschlossen**, folgende Stellungnahme im gegenständlichen Konsultationsverfahren abzugeben:

II. Überlegungen zur Mitteilung der Kommission

A. Globale Betrachtungen / Überblick

Die Kommission geht in ihrer Mitteilung grundsätzlich davon aus, dass Datenschutz und der Schutz der Privatsphäre auf Grund der raschen technischen Entwicklungen und der Globalisierung vor neuen Herausforderungen steht und *Anpassungen erforderlich* sind. **„Die *wesentlichen Grundsätze* der Datenschutz-Richtlinie (kurz: DSRL) *sollen* (jedoch) *nach wie vor Gültigkeit haben* und ihre Technikneutralität beibehalten werden“** (vgl. Seite 3 ff Mitteilung). Diese Feststellung der Kommission ist mit Nachdruck zu unterstützen, ebenso wie das angestrebte Ziel

der Beibehaltung eines *„hohen Schutzniveaus für den Einzelnen bei der Verarbeitung personenbezogener Daten“* (vgl. Seiten 5, 21 der Mitteilung).

Uneingeschränkt zuzustimmen ist der Kommission auch hinsichtlich ihrer Diagnose zunehmender Gefahren für die Privatsphäre durch die immer weiter ausgreifende **Nutzung von Internet-basierten oder besser „Online“-Technologien** (Stichworte: „Soziale Netzwerke“, „Cloud Computing“ etc.) bzw. Anwendungen zur drahtlosen Datenübertragung (Mobilfunk jeweils in Verbindung mit Verfahren der automatisierten elektronischen Standortbestimmung oder RFID-Technologien stützen; Bsp: elektronische Mautsysteme, elektronische Tickets in öffentlichen Verkehrsmitteln etc.; vgl. Seiten 2 ff der Mitteilung).

Zur konkreten *Beantwortung* der *Frage,* wie die *Auswirkungen* der genannten Technologien datenschutzrechtlich *beherrschbar* gemacht werden können (vgl. Seite 3 der Mitteilung), *trägt die Mitteilung* der Kommission selbst *allerdings nur bedingt bei.* Vom Verweis auf das bestehende Instrument der Telekom-Datenschutzrichtlinie (2002/58/EG) abgesehen (vgl. Seite 3 der Mitteilung) beschränkt sich die Kommission darauf einzelne, zweifelsohne wichtige Aspekte anzusprechen (etwa: verständliche Informationen der Betroffenen [Seite 6 der Mitteilung], Kontrolle über die „eigenen Daten“ im Rahmen von sozialen Online-Netzwerken [Seite 8 der Mitteilung], Präzisierung der Regelungen über die „Einwilligung“ [Seite 9 der Mitteilung] oder „anwenderfreundlichere“ Gestaltung der Regelungen über das anwendbare Datenschutzrecht [Seite 12 der Mitteilung]).

Andere wichtige *praktische Probleme,* die sich vor allem im Rahmen der Internetnutzung stellen bleiben dagegen ausgeklammert oder werden nicht ausreichend gewürdigt. Zu verweisen ist hier etwa auf Fragen des Datamining und Profiling, wie sie sich sowohl innerhalb als auch außerhalb des Internets ergeben.

Die zentrale legistische Grundsatzfrage, die sich mit Blick auf ergänzende, präzisierende Regelungen zur Lösung obgenannter Probleme stellt, ist jene nach dem richtigen „Ort“. Mit anderen Worten: Sollen die Konkretisierungen der allgemeinen Grundsätze direkt in der allgemeinen Datenschutzrichtlinie erfolgen oder in bereichsspezifischen Instrumenten? Wie das Muster der „Telekom-Datenschutzricht-

linie“ (2002/58/EG) zeigt, dürfte letzterer Option in der Regel der Vorzug zu geben sein.

Ungelöste praktische Fragen, insbesondere in Form von ***Auslegungsfragen*****,** stellen sich weiterhin in Bezug auf Daten, die mittels *bildgebender technischer Verfahren* gewonnen werden (Stichwort: Videoüberwachung im „öffentlichen Raum“). So ist nicht im Letzten klar, ob bzw. unter welchen Voraussetzungen solche Daten als „sensible“ Daten im Sinne des Art. 8 Abs. 1 der Datenschutzrichtlinie zu qualifizieren sind.

Ein bis dato von der Datenschutzrichtlinie nicht gelöstes Problem ist auch die Frage der ***Transparenz*** **grenzüberschreitender Informationsverbundsysteme**. Bei solchen Datenanwendungen mit mehreren datenschutzrechtlichen Auftraggebern mit Sitz in verschiedenen Mitgliedstaaten stellt sich konkret die Frage, wie in den einzelnen Mitgliedstaaten im Zuge allfälliger Registrierungsverfahren vorzugehen ist. Der derzeitige Rahmen der Richtlinie (Art. 18 ff) geht erkennbar von einer rein lokalen Betrachtungsweise aus. Mit der verfahrensmäßigen Behandlung grenzüberschreitender Informationsverbundsysteme eng zusammenhängend ist die von der Kommission angedachte *Vereinfachung der derzeitigen Melderegelung* (vgl. Seite 12 der Mitteilung). Die Aussagen der Mitteilung zu diesem Thema bleiben freilich sehr vage.

Die Betonung des Prinzips der ***Datensparsamkeit*** (vgl. Seite 8) 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 Nachdruck zu unterstützen ist das Bemühen der Kommission, ***aufklärende Maßnahmen*** zu setzen, die insbesondere das Risikobewusstsein junger Menschen erhöhen sollen (vgl. Seite 9 der Mitteilung). Zugleich sei angemerkt, dass solche Schritte im Grunde jenseits des regulatorischen Bereiches liegen und sich daher nur

bedingt in künftigen Rechtsinstrumenten niederschlagen können (allenfalls in Zielbestimmungen). Im Rahmen der Einführung neuer legistischer Maßnahmen sollen verstärkt bewusstseinsfördernde Maßnahmen über bestehende Rechte angeboten und umgesetzt werden.

Differenziert zu sehen sind die Überlegungen der Kommission zur in Aussicht genommenen ***Einstufung zusätzlicher Datenkategorien als „sensible Daten"*** (vgl. Seite 11 der Mitteilung). Dazu wird auf die nachfolgenden Detailbemerkungen verwiesen.

Zu den Ausführungen der Kommission zur ***„Binnenmarktdimension"* des Datenschutzes** ist zu sagen, dass es zutrifft, dass ein zentrales Motiv hinter der Erlassung der Datenschutzrichtlinie in der Erreichung eines *„freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten"* war (vgl. Seite 11 der Mitteilung). **Zu betonen ist allerdings, dass durch das Inkrafttreten der Grundrechtecharta der EU neben dem Binnenmarktziel auch die Gewährleistung der Privatsphäre bzw. des Datenschutzes ihre ausdrückliche Verankerung im Primärrecht gefunden haben.** Damit hat sich zugleich der primärrechtliche Prüfungsmaßstab, der an Sekundärrechtsakte wie die DSRL und verwandte Instrumente anzulegen ist, deutlich erweitert. Es müssen insofern die Marktfreiheiten als auch die Grundrechte gleichermaßen ins Kalkül gezogen werden.

Unbeschadet des grundsätzlich legitimen Ziels der Verwaltungsvereinfachung erschiene es geboten zu prüfen, ob und inwieweit bestimmte ***besonders eingriffsintensive Verfahren der Datenverwendung*** einer Art Vorabkontrolle unterworfen werden sollten.

Zur von der Mitteilung angesprochenen ***Selbstregulierung*** (vgl. Seite 14) ist anzumerken, dass diese zur Voraussetzung hat, dass *sämtliche* Akteure eine konstruktive Haltung einnehmen und datenschutzkonformen/-fördernden und praktikablen Lösungen gegenüber aufgeschlossen sind.

Mit Nachdruck zu begrüßen ist hingegen 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 polizei-

lichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, nur als erster Schritt gesehen werden, dessen *Defizite* die Kommission *vollzutreffend anführt* (v.a. keine Geltung für rein nationale Verarbeitungen für die besagten Zwecke, zu viele Ausnahmen vom Zweckbindungsgrundsatz; vgl. Seite 15 der Mitteilung).

Zu begrüßen ist schließlich die in der Mitteilung vorgenommene kritische Auseinandersetzung mit der Frage des ***„Datenexports" in Drittstaaten*** (vgl. Seiten 17 ff). 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).

Der österreichische Datenschutzrat hat am 26. Februar 2010 sehr ausführlich gegenüber der Kommission im Rahmen des öffentlichen Konsultationsverfahrens zum geplanten Abkommen mit der US-Regierung über den Austausch personenbezogener Daten zu Strafverfolgungszwecken Stellung genommen. Unsere damals dargelegten Positionen sollen auch als Teil unserer Stellungnahme zu dieser Mitteilung der Kommission verstanden werden.

Erwägenswert erschiene es im Übrigen, in ein künftiges Instrument zum allgemeinen Datenschutz ausdrückliche Regelungen über sog. ***pseudonymisierte Daten*** (auch: „indirekt personenbezogenen" Daten) aufzunehmen. Damit ist eine Kategorie von Daten angesprochen, bei der in einem Datensatz die zur Identifizierung einer bestimmten Person geeigneten Daten durch ein Pseudonym ersetzt werden, wobei die Information über die Zuordnung Ersterer zu Letzteren außerhalb des Datensatzes gespeichert wird. Nur wer über diesen separierten „Schlüssel" verfügt ist in der Lage, den Datensatz auf eine bestimmte Person rückzuführen. Die übrigen Verwender des Datensatzes können dagegen den Personenbezug nicht herstellen. Für diese können insofern deutlich erleichterte, privilegierende Datenverwendungsregelungen gelten.

In ***Österreich*** hat das Konzept der indirekt personenbezogenen Daten seinen ausdrücklichen Niederschlag im (allgemeinen) Datenschutzgesetz 2000 (BGBl. I

Nr. 165/1999 i.d.F. BGBl. I Nr. 133/2009) gefunden (vgl. die Legaldefinition in § 4 Z 1 und diverse Privilegierungen in § 8 Abs. 2, § 9 Z 2, § 12 Abs. 3 Z 2, § 17 Abs. 2 Z 3, § 29, § 46 Abs. 1 Z 3).

Die Mitglieder des Datenschutzrates sind überwiegend der Meinung, dass besonderes Augenmerk auch darauf gelegt werden sollte, welche Konsequenzen sich aus dem Umstand ergeben, dass im Zuge vieler interaktiver Datenanwendungen vordergründig zwar lediglich Daten über eine bestimmte technische Einrichtung (Bsp: Maschinennummer von „Smartphone“ oder „Laptop“) erhoben und weiterverarbeitet werden, diese Daten letztlich aber über die faktische Bindung an einen bestimmten Gerätebesitzer/-nutzer sehr wohl einen Personenbezug aufweisen.

B. Bemerkungen zu den einzelnen Abschnitten der Mitteilung

Zu Abschnitt 2.1. Stärkung der Rechte des Einzelnen

2.1.1. Angemessener Schutz des Einzelnen in allen Situationen

Die Kommission zieht dazu folgenden Schluss (Seite 6 der Mitteilung):

> 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.**

Aus der Sicht des Datenschutzrates ist dazu anzumerken:

- Vordringlicher Handlungsbedarf unter dem Gesichtspunkt des Individualrechtsschutzes besteht im Bereich der *Internetnutzung* durch User. Folgende Problemfelder könnten einer Überprüfung im Hinblick auf regulatorische Schritte unterzogen werden:
  - ***Funktionalitäten von Suchmaschinen (***Stichworte: Möglichkeiten für Nutzer, gezielt Einfluss auf die Weiterverarbeitung der über ihr Suchverhalten anfallenden Daten nach Abschluss einer Suche bzw. „Sitzung“ zu nehmen; Problematik der Sanktionierung der Nichteinhaltung allfälliger Vorgaben).
  - ***„Profilbildung“*** **mittels im Internet verfügbarer Daten.**
  - ***Informationspflichten*** **von Online-Diensteanbietern gegenüber Nutzern** (siehe dazu auch unten in Abschnitt 2.1.2).

- ***Grundsätzliche Rechtsstellung von Nutzern* von sozialen Online-Netzwerken gegenüber den Anbietern einschlägiger Plattformen** (Stichwort: Reichweite der Rechte der Nutzer auf Änderung oder vollständige Löschung ihrer Daten?).
- **Verankerung des Grundsatzes,** dass **Angebote an die Konsumenten in einer Weise zu erfolgen haben, dass diese** – wann immer es die Natur der zu erbringenden Leistung zulässt (Bsp: Lösen von Fahrscheinen, Konsumation von Informationen im Internet) – **anonym in Anspruch genommen werden können.** Zudem müsste gewährleistet sein, dass auf die Konsumenten **kein überproportional indirekter Druck zur freiwilligen Aufgabe ihrer Anonymität ausgeübt wird.**
- **Reflexion der Pflicht zur Vorratsdatenspeicherung** nach der Richtlinie 2006/24/EG, insbesondere im Kontext des freien Informationszugangs mittels Internet.
- **Prüfung der Möglichkeit der Stärkung von Initiativen der Zivilgesellschaft, die auf die datenschutzkonforme Gestaltung des Online-Sektors abzielen** (z.B. E-Commerce-Gütesiegel oder Privacy-Audit).

- Falls die Überlegungen zu den oben angesprochenen Punkten zur Notwendigkeit von Regulierungen führen sollten, müsste man sich über den Ort dieser Regelungen Gedanken machen. Die bereits existierenden Datenschutzrichtlinien (allgemeine Datenschutzrichtlinie und „Telekom-Datenschutzrichtlinie) sollten damit nicht überfrachtet werden. Es wäre zu prüfen, ob derartige Regelungen in bestehende materienspezifische Sekundärrechtsakte aufgenommen werden sollen, oder ob diese in einem eigenen, für spezifische Dienste zu schaffenden Sekundärrechtsakt geregelt werden sollen.
- Angezeigt erscheint auch eine Befassung mit der Frage der wirksamen Anwendung der **allgemeinen Datenschutzgrundsätze** auf die Verarbeitung von **Nutzungsdaten, die etwa im Rahmen von *Kundenbindungsprogrammen, im spezifischen Feld der Kommunikationsdienst-***

- Besonderes Augenmerk ist weiters auf den Umgang mit **„Standortdaten" bzw. „Geodaten"** zu richten (z.B. Weiterverwendung von personenbezogenen Standortdaten).
- Besitzer von Immobilien (ausgenommen historische bzw. staatliche Immobilien) sollten das Recht erhalten, der fotographischen Reproduktion ihrer Immobilie im Rahmen von auf Geodaten basierten Online-Angeboten, die eine Identifizierung des Besitzers/Nutzers der Immobilie ermöglichen, zu widersprechen. Von dieser Widerspruchsmöglichkeit ausgenommen wäre das Recht auf Freiheit des Straßenbildes nach urheberrechtlichen Bestimmungen.
- Spezifischer Überprüfung bedarf auch die Frage des Regelungsbedarfs in Bezug auf den **Einsatz bildgebender Verfahren zu Überwachungszwecken** („Videoüberwachung"), sei es durch Private, sei es durch staatliche Stellen (Stichworte: Definition höchstpersönlicher Lebensbereiche, die jedenfalls von Überwachung frei bleiben müssen; uneingeschränkte Geltung des Verhältnismäßigkeitsprinzips).

2.1.2. Mehr Transparenz für die von der Verarbeitung Betroffenen

Die Kommission zieht dazu folgende Schlüsse (Seite 7 der Mitteilung):

> 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.

Aus der Sicht des Datenschutzrates ist dazu anzumerken, dass die Verbes¬serung der Transparenz vor allem im Online-Bereich vordringlich erscheint. Dabei sollte überlegt werden, ob im Bereich der Online-Dienste (z.B. Social Networks, Social Media oder WEB 2.0) bezüglich der Verwendung

personen¬bezogener Informationen transparente Lösungen angeboten werden sollen (gleichberechtigt opt-in oder opt-out).

Diese Frage ist auch im Offline-Bereich von praktischer Relevanz.

Über die vorstehend angesprochene Perspektive der Internetnutzung hinaus stellen sich Transparenzfragen auch zunehmend als Folge der Vernetzung von Objekten („Internet der Dinge“).

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 Vorgangsweise wird vom Datenschutzrat unterstützt, zumal im öster¬reichischen Datenschutzgesetz eine derartige Regelung bereits vorge¬sehen ist.

2.1.3. Bessere Kontrolle des Betroffenen über seine Daten

Die Kommission zieht dazu folgende Schlüsse (Seite 8 der Mitteilung):

Die Kommission wird daher Möglichkeiten prüfen, um

- das **Prinzip der Datensparsamkeit** zu stärken;

- die **Modalitäten** für die **Wahrnehmung der Rechte auf Zugang zu Daten, auf deren Berichtigung, Löschung oder Sperrung** zu verbessern (z.B. durch Einführung einer Antwortfrist für diesbezügliche Anträge, durch Zulassung technischer Lösungen, mit denen die Rechte auf elektronischem Weg wahrgenommen werden können, oder durch eine Vorschrift, wonach das Zugriffsrecht grundsätzlich gebührenfrei zu gewähren ist);

- das sogenannte **Recht auf Vergessen („right to be forgotten“)** zu präzisieren, also das Recht von Personen, dass ihre Daten nicht länger verarbeitet und gelöscht werden, wenn sie nicht mehr für einen rechtmäßigen Zweck gebraucht werden. Dies ist beispielsweise der Fall, wenn die Verarbeitung auf der Grundlage der Zustimmung einer Person zur Verarbeitung erfolgt und wenn diese Person ihre Zustimmung zurückzieht oder wenn die Vorhaltefrist abgelaufen ist;

- die Rechte des von der Verarbeitung Betroffenen zu erweitern, in dem die **„Datenübertragbarkeit“** sichergestellt wird, also das Recht des Einzelnen, seine Daten (z. B. Fotos oder Freundeverzeichnisse) auf einer Anwendung oder einem

Dienst zurückzuholen und die zurückgeholten Daten auf eine andere Anwendung oder einen anderen Dienst zu übertragen, sofern dies technisch möglich ist, ohne von dem für die Verarbeitung Verantwortlichen daran gehindert zu werden.

Aus der Sicht des Datenschutzrates ist dazu anzumerken:

In Bezug auf den Grundsatz der Datensparsamkeit ist an dieser Stelle auf die korrespondierenden Ausführungen im Abschnitt II.A zu verweisen. Hinsichtlich des Zugriffsrechts auf die „eigenen Daten“ in Online-Umgebungen wie sozialen Netz¬werken oder vergleichbaren Anwendungen ist auf einschlägige Ausführungen oben in Abschnitten II.A und II.B.2.1.1. zu verweisen. Ergänzend dazu ist festzuhalten, dass es hinsichtlich des Zugriffsrechts des/der Betroffenen auf „eigene Daten“ in der Praxis einer Differenzierung zwischen verschiedenen Anwendungen bedarf. So kann es beispielsweise in der Regel keinen unmittelbaren Zugriff auf in behördlichen Verfahrens¬akten gespeicherte Daten Betroffener geben. Wohl aber sind Weiter¬entwicklungen in Bezug auf die beschleunigte Online-Kommunikation zwischen Bürger und Behörde sinnvoll.

Auch die Handhabung von Verfallsdaten stellt sich im Einzelnen komplex dar. Hier bedarf es tiefergehender Überlegungen. An dieser Stelle darf angemerkt werden, dass das „Recht auf Vergessen“ eine umso geringere Rolle spielt, je mehr gerade im Online-Bereich an anonymen Nutzungsmöglichkeiten bereitsteht.

Die Frage der leicht(eren) Übertragbarkeit von persönlichen Daten von einer Anwendung auf eine andere stellt kein vorrangiges Datenschutzproblem dar.

2.1.4. Bewusstsein fördern

Die Kommission zieht dazu folgende Schlüsse (Seite 9 der Mitteilung):

Die Kommission wird Folgendes sondieren:

- die Möglichkeit der **Kofinanzierung von Aufklärungsmaßnahmen zum Thema Datenschutz** mit Mitteln aus dem EU-Haushalt;

- die Notwendigkeit einer einschlägigen Verpflichtung in der Datenschutzregelung zu **Aufklärungsmaßnahmen** und die Möglichkeiten, die die Regelung dazu bietet.

Diese Position wird vom Datenschutzrat ausdrücklich unterstützt. Medienpädagogik – Aufklärung über Chancen und Risiken des Internets - muss institutionalisiert und in den schulischen Unterricht, die Aus- und Weiterbildung der Lehrer sowie in die Erwachsenenbildung integriert werden. Datenschutz und Schutz der Privatsphäre muss eine zentrale Bildungsaufgabe werden. Dafür sollen auch entsprechende finanzielle Mittel bereit gestellt werden.

2.1.5. Gewährleistung der Einwilligung ohne Zwang und in Kenntnis der Sachlage
Die Kommission zieht dazu folgenden Schluss (Seite 10 der Mitteilung):

Die Kommission wird prüfen, wie **die Bestimmungen über die Einwilligung präzisiert und gestärkt werden können.**

Diese Vorgangsweise wird vom Datenschutzrat ausdrücklich unterstützt. Zugleich wird auf die korrespondierenden Ausführungen zum Online-Bereich oben in den Abschnitten 2.1.1. und 2.1.2 verwiesen.

2.1.6. Schutz sensibler Daten
Die Kommission zieht dazu folgende Schlüsse (Seite 10 der Mitteilung):

Die Kommission wird prüfen, - ob andere Datenkategorien, beispielsweise **Gendaten**, als **sensible Daten** eingestuft werden sollten; - ob die **Voraussetzungen** für die Zulassung der Verarbeitung bestimmter Kategorien sensibler Daten **präzisiert und harmonisiert** werden sollten.

Dazu merkt der Datenschutzrat an, dass „Gendaten“, sofern damit menschliche DNA-Daten gemeint sind, differenziert zu sehen sind. Soweit es um sog. kodierende Teile der DNA geht, sind diese wohl schon heute als gesundheitsbezogene und damit sensible Daten anzusehen. Eine umfassende Auflistung sämtlicher sensibler Daten im Sinne von Art. 8 der Datenschutzrichtlinie erschiene im Übrigen nicht realistisch und zweckmäßig. Überlegungen sollten aber dahin angestellt werden, wie sichergestellt werden kann, dass sensiblen Daten durchaus ver-

gleichbare Daten wie etwa über strafrechtliche Verurteilungen ausreichend geschützt werden können.

2.1.7. Wirksamere Rechtsbehelfe und Sanktionen

Die Kommission zieht dazu folgende Schlüsse (Seite 10 der Mitteilung):

> 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.

Die europaweite Harmonisierung bei Sanktionsregelungen ist auch aus Sicht des Datenschutzrates prüfenswert. Auch das „Stockholm-Programm" verlangt eine konsequente Anwendung des Grundrechts auf Datenschutz in allen Mitgliedstaaten.

Zu Abschnitt 2.2. Stärkung der Binnenmarktdimension

2.2.1. Mehr Rechtssicherheit und gleiche Bedingungen für die Verantwortlichen für die Datenverarbeitung

Die Kommission zieht dazu folgenden Schluss (Seite 11 der Mitteilung):

> Die Kommission wird Ansätze für eine **weitere Harmonisierung der Datenschutzbestimmungen auf EU-Ebene** prüfen.

Diese Vorgangsweise wird vom Datenschutzrat unterstützt. Hinsichtlich potentieller Harmonisierungsbereiche wird wiederum auf die Ausführungen in den Abschnitten II.A und II.B.2.1.1. verwiesen. Weiters sollte auch die Ausweitung des Geltungsbereichs der allgemeinen Datenschutzrichtlinie auf juristische Personen geprüft werden.

2.2.2. Verringerung des Verwaltungsaufwands

Die Kommission zieht dazu folgenden Schluss (Seite 12 der Mitteilung):

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

Diese Vorgangsweise wird vom Datenschutzrat unterstützt. Ebenso wird der Vorschlag der Kommission unterstützt, die derzeitigen Melderegelungen zu vereinfachen (unter der Bedingung dass die Aufrechterhaltung eine hohen datenschutzrechtlichen Niveaus gewährleistet wird) und alternative Möglichkeiten zu Meldeverfahren zu prüfen.

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

Die Kommission zieht dazu folgenden Schluss (Seite 12 der Mitteilung):

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.

In diesem Kontext erlaubt sich der Datenschutzrat auf folgendes hinzuweisen:

In seiner Stellungnahme vom 21. Jänner 2010 hat er darauf darauf hingewiesen, dass auf Grund der Regelungen in Art. 4 Abs. 1 der DS-RL (welche insb. im § 3 DSG 2000 auf nationaler Ebene umgesetzt wurden) Beschwerden von Betroffenen gegen Datenschutzverletzungen durch einen Website-Betreiber, dessen Niederlassungen sich in einem anderen EU-Mitgliedstaat befinden, bei der dort ansässigen Daten¬schutzbehörde geltend gemacht werden (z.B. Beschwerden gegen das Aufnehmen und Fotografieren des öffentlichen Raums in Österreich durch einen rumänischen Datenverarbeiter [www.norc.at] bei der rumänischen Datenschutzbehörde). Diese Rechts¬lage erscheint dem Datenschutzrat unzumutbar, weil der Beschwerdeführer gezwungen wird, sich Kenntnis über das jeweilige ausländische Datenschutzrecht zu verschaffen, was aber notwendig ist, um festzustellen, welche Rechtsmittel auch im ordentlichen Rechtsweg möglich sind.

Dies impliziert wiederum, dass der Be¬schwerde¬führer wohl einen Rechtsanwalt heranziehen muss.

Der Datenschutzrat regt daher an, im Rahmen des neuen umfassenden Rechts¬rahmens 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 und diese auch das inländische Recht anwendet. Diesbezüglich liegt auch ein einstimmiger Beschluss des österreichischen Nationalrates vor.

2.2.4. Mehr Verantwortung der für die Verarbeitung Verantwortlichen

Die Kommission zieht dazu folgende Schlüsse (Seite 14 der Mitteilung):

> Die Kommission wird folgende Maßnahmen prüfen, um die Verantwortung der für die Verarbeitung Verantwortlichen zu stärken:
>
> – verpflichtende Benennung eines unabhängigen **Datenschutzbeauftragten** und Harmonisierung der Bestimmungen über dessen Aufgaben und Zuständigkeiten, wobei zur Vermeidung eines übermäßigen Verwaltungsaufwands vor allem für kleine und kleinste Unternehmen angemessene Schwellen in Erwägung zu ziehen wären;
>
> – Einführung – in der Datenschutzregelung – der Pflicht der für die Verarbeitung Verantwortlichen zur Durchführung einer **Datenschutzfolgenabschätzung** in bestimmten Fällen, wenn beispielsweise sensible Daten verarbeitet werden oder wenn die jeweilige Verarbeitung mit besonderen Risiken verbunden ist, insbesondere beim Einsatz bestimmter Technologien, Systeme und Verfahren, darunter bei der Erstellung von Profilen oder Videoüberwachung;
>
> – weitere Förderung von Technologien zum Schutz der Privatsphäre und der Möglichkeiten für die konkrete Umsetzung des **Privacy-by-Design**-Konzepts.

Diese Vorgangsweise wird vom Datenschutzrat hinsichtlich des Privacy-by-Design-Konzepts grundsätzlich unterstützt. Im Hinblick auf die Prüfung der verpflichtenden Benennung von unabhängigen Datenschutzbeauftragten wird daran erinnert, dass es Art. 18 der DSRL derzeit den Mitgliedstaaten anheim stellt, entweder eine Meldung der Datenanwendung an eine Kontrollstelle oder stattdessen die Bestellung eines betrieblichen Datenschutzbeauftragten

vorzu¬sehen. Von ersterer haben zahlreiche Mitgliedstaaten, so auch Öster¬reich, Gebrauch gemacht und auch entsprechende Strukturen bei der Kontrollstelle errichtet sowie dafür Investitionen getätigt.

Zum Thema Datenschutzfolgeabschätzungen vertritt der Datenschutzrat die Auffassung, dass diese keinesfalls zu unverhältnismäßigen Kosten und bürokratischen Erfordernissen führen sollten.

2.2.5. Förderung von Initiativen zur Selbstregulierung und Möglichkeit der Zertifizierung durch die EU

Die Kommission zieht dazu folgende Schlüsse (Seite 14 der Mitteilung):

Die Kommission wird

- Möglichkeiten zur **verstärkten Förderung von Initiativen zur Selbstregulierung** prüfen, darunter die aktive Förderung von Verhaltenskodizes.

- die Möglichkeit der Einführung von **EU-Zertifizierungsregelungen** für den Schutz der Privatsphäre und den Datenschutz sondieren.

Diese Vorgangsweise wird vom Datenschutzrat unterstützt. Allerdings sollte die Anwendung von EU-Zertifizierungsregelungen auf freiwilliger Basis beruhen.

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

Die Kommission zieht dazu folgende Schlüsse (Seite 17 der Mitteilung):

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.

Der Datenschutzrat unterstützt nachdrücklich 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.

Hinsichtlich der „Gendaten“ wird auf die Ausführungen in Abschnitt 2.1.6. verwiesen.

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.

Erwägenswert wäre auch die ausdrückliche Verankerung eines allgemeinen Grundsatzes, wonach verdachtsunabhängige Überwachungsmaßnahmen, die die Bevölkerung insgesamt bzw. eine gesamte soziale Gruppe treffen und auf die Wiedererkennbarkeit jedes einzelnen Betroffenen abzielen, nur auf entsprechender gesetzlicher Grundlage, auf den Einzelfall begrenzt, für genau definierte Zwecke und unter Einhaltung entsprechender, der Wahrung der Verhältnismäßigkeit dienender verfahrensrechtlicher Sicherungen in Betracht kommen können.

Der Österreichische Datenschutzrat verweist in diesem Zusammenhang wieder auf die Stellungnahme, die im Rahmen des öffentlichen Konsultationsverfahrens zum geplanten Abkommen mit der US-Regierung über den Austausch von personenbezogenen Daten zu Strafverfolgungszwecken abgegeben wurde (siehe Anhang).

Zu Abschnitt 2.4. Die globale Dimension des Datenschutzes

2.4.1. Klärung und Vereinfachung der Bestimmungen über internationale Datentransfers

Die Kommission zieht dazu folgende Schlüsse (Seite 18 f der Mitteilung):

Die Kommission wird prüfen, wie

- die **bestehenden Verfahren** für den internationalen Datentransfer, darunter rechtsverbindliche Instrumente und verbindliche unternehmensinterne Vorschriften, **verbessert und koordiniert** werden können, um ein **einheitlicheres und kohärenteres Vorgehen der EU** gegenüber Drittländern und internationalen Organisationen sicherzustellen;

- das **Verfahren der Kommission zur Prüfung der Angemessenheit präzisiert** und geeignete **Kriterien und Anforderungen** für die Bewertung des Datenschutzniveaus in einem Drittland oder in einer internationalen Organisation festgelegt werden können;

- wie die **zentralen Elemente des Datenschutzes** zu definieren sind, die für alle Arten von internationalen Übereinkommen verwendet werden können.

Diese Vorgangsweise wird vom Datenschutzrat ausdrücklich unterstützt.

2.4.2. Förderung universeller Grundsätze

Die Kommission zieht dazu folgende Schlüsse (Seite 19 f der Mitteilung):

Die Kommission wird

- sich weiterhin **für die Festlegung hoher rechtlicher und technischer Datenschutzstandards** in Drittländern und auf internationaler Ebene **einsetzen**;

- sich auf internationaler Ebene für den **Grundsatz der Gegenseitigkeit des Schutzes** einsetzen, vor allem beim Export von Daten der von der Verarbeitung Betroffenen aus der EU in Drittländer;

- **dazu enger mit Drittländern und internationalen Organisationen zusammenarbeiten**, darunter mit der OECD, dem Europarat, den Vereinten Nationen und anderen regionalen Organisationen;

- **die Entwicklung internationaler technischer Normen durch Normungsorganisationen** wie CEN und ISO **aufmerksam verfolgen**, um sicherzustellen, dass diese die Rechtsvorschriften sinnvoll ergänzen und die Umsetzung und wirksame Anwendung der wichtigsten Datenschutzvorschriften gewährleisten helfen.

Diese Vorgangsweise wird vom Datenschutzrat ausdrücklich unterstützt. Gewährleistet werden muss, dass mit der Entwicklung neuer technischer Normen rechtliche Datenschutzstandards nicht unterlaufen werden (z.B. ETSI-Standards).

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

Die Kommission zieht dazu folgende Schlüsse (Seite 20 f der Mitteilung):

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.**

Diese Vorgangsweise wird vom Datenschutzrat ausdrücklich unterstützt.

III. Überlegungen über die Mitteilung hinaus mit Bezug zum institutionellen Rahmen der EU

Die in den vorstehenden Abschnitten diskutierte Mitteilung der Kommission zielt primär auf legistische bzw. begleitende nichtlegistische Maßnahmen ab, die die Mit¬gliedstaaten binden sollen. Im Lichte der Anforderungen der Art. 7 und 8 der Grund¬rechte¬charta bzw. gerade auch mit Blick den im Vorabschnitt kritisch angemerkte Beispiele für höchst problematische geplante Gesetzesinitiativen erscheint es jedoch auch geboten, Überlegungen dahingehend anzustellen, wie künftig sichergestellt werden kann, dass die EU-Sekundärrechtsetzung selbst datenschutzkonform erfolgt. In diesem Kontext sind u.a. interne Abläufe sowohl in Kommission als auch im Rat angesprochen.

So erschiene es zweckmäßig, mit Gesetzesinitiativen mit Auswirkungen auf das Datenschutzgrundrecht nicht nur die primär facheinschlägige Ratsarbeitsgruppe zu befassen, sondern zusätzlich die Ratsarbeitsgruppe „Datenschutz und Informations¬austausch“. Letztere sollte auf Basis ihrer spezifischen Expertise die datenschutz¬relevanten Aspekte jedes vorgeschlagenen EU-Rechtsaktes beraten und insofern die Arbeit der federführenden Ratsarbeitsgruppe unterstützen. Technisch gesehen wäre eine solche Vorgangsweise durch einen Beschluss des sog. Ausschusses der Ständi¬gen Vertreter (AStV; vgl. Art. 19 der Geschäftsordnung des Rates) festzu¬legen. Analog dazu sollte auch innerhalb der Kommission – sofern nicht bereits praktisch umgesetzt – auf Fachebene eine verpflichtende Konsultierung der mit Fragen der Datenschutzlegistik befassten Abteilung vorgesehen werden, bevor einschlägige datenschutzrelevante Vorschläge für Rechtsakte angenommen werden.

In Erwägung gezogen werden sollte auch eine Weiterentwicklung des Mandats der Agentur der Europäischen Union für Grundrechte. So erschiene es wünschenswert, wenn die Agentur über ihre unterstützende, beratende Rolle beim grundrechts¬kon¬formen Vollzug von Gemeinschaftsrecht hinaus ihre unabhängige Grundrechts¬expertise bereits auf der Stufe der Vorstellung europäischer Gesetzesinitiativen einbringen könnte.

Beilage – Stellungnahme des Datenschutzrates vom 26.2.2010

27. Jänner 2011
Für den Datenschutzrat:
Der Vorsitzende:
MAIER

Elektronisch gefertigt