A-1010 Wien, Hohenstaufengasse 3

Tel. ++43-1-531 15/0

Fax: ++43-1-531 15/2690

e-mail: dsk@dsk.gv.at

DVR: 0000027

REPUBLIK ÖSTERREICH

DATENSCHUTZKOMMISSION

GZ: DSK-K053.000/0002-DSK/2010

An die Europäische Kommission
Generaldirektion Justiz und Grundrechte

Referat C3 – Datenschutz
B - 1049 Brüssel

per E-Mail: JUST-PRIVACY-CONSULTATIONS@ec.europa.eu

Betrifft: Mitteilung der Kommission an das Europäische Parlament und den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Gesamtkonzept für den Datenschutz in der Europäischen Union

Die österreichische Datenschutzkommission nimmt im Rahmen des Konsultationsverfahrens zur im Betreff genannten Mitteilung der Europäischen Kommission wie folgt Stellung:

Zu Kapitel 1. *Neue Herausforderungen für den Datenschutz*

Die Datenschutzkommission begrüßt die Ausarbeitung eines neuen Rechtsinstruments, sofern durch dieses ein **hoher Datenschutzstandard** gewährleistet wird und der durch die Richtlinie 95/46/EG gesetzte Standard nicht unterschritten wird. Die Datenschutzkommission teilt die Meinung, dass neue Herausforderungen wie **neue Technologien**, aber auch die **mangelnde Harmonisierung** in Bereichen des Datenschutzes ein umfassendes kohärentes Konzept, das die lückenlose Einhaltung des Grundrechts des Einzelnen auf Schutz seiner Daten in der EU und in Drittstaaten garantiert, erforderlich machen.

Eine mangelnde Harmonisierung besteht zum Beispiel im Bereich der **Videoüberwachung**. So werden etwa Daten aus Videoaufzeichnungen in vielen Mitgliedstaaten grundsätzlich als

nicht sensibel gewertet, obwohl man bei strenger Interpretation des Art. 8 der RL 95/46/EG auch zum Schluss kommen könnte, dass jede Videoaufzeichnung und jedes Foto sensible Daten enthält, weil immer rassische und ethnische Merkmale von Menschen feststellbar sind oder Rückschlüsse auf die Gesundheit oder (unter Umständen) religiöse Zugehörigkeit von Personen möglich sein können. Es wäre anzudenken, Spezialbestimmungen für den Bereich der Verwendung von Bilddaten, aber eventuell auch **für andere besondere Technologien oder Verfahren** (z B. RFID, „Profiling“) zu schaffen.

Gleiches gilt auch für die Prinzipien des **Datenschutzes** im Zusammenhang mit **Arbeitsverhältnissen**. Auch hier lässt die mangelnde Harmonisierung zwischen den Rechtsordnungen der Mitgliedstaaten ein unterschiedlich hohes Schutzniveau für Arbeitnehmer und Arbeitnehmerinnen entstehen, das gerade im Zusammenhang mit der Internationalisierung auch des Arbeitsverhältnisses aus der Sicht des Betroffenen problematisch scheint.

Ein Mangel an Harmonisierung ist insbesondere im Bereich der **Ausgestaltung, Ausstattung und der Kompetenzen der Datenschutzbehörden** festzustellen. Die Datenschutzkommission teilt hiezu die Meinung der Europäischen Kommission, dass die Datenschutzbehörden mehr Befugnisse erhalten sollten, damit die Einhaltung der Datenschutzvorschriften besser durchgesetzt werden kann. Dies kann jedoch nur mit einer dementsprechenden Ausstattung der Datenschutzbehörden einhergehen (siehe dazu die Ausführungen zu Punkt 2.5.).

Zu 2.1.1*. Angemessener Schutz des Einzelnen in allen Situationen*

Bezüglich des Konzeptes der „personenbezogenen Daten“ wird darauf hingewiesen, dass auch hinsichtlich der Verwendung „**pseudonymisierter Daten**“ (also jener Daten, die für denjenigen, der sie verwendet, nicht auf eine Person rückführbar sind, obwohl sie nicht generell anonymisiert wurden) keine ausreichende Harmonisierung besteht. In den meisten Mitgliedstaaten fehlen Regelungen über die Verwendung dieser Daten. Mitunter werden solche Daten als nicht personenbezogen betrachtet, während es sich dabei aber aus Sicht der Datenschutzkommission um personenbezogene Daten handelt. Die Verwendung von pseudonymisierten Daten hat sich insbesondere im Bereich der sensiblen Daten, etwa der Verwendung von medizinischen Daten für Forschungszwecke oder der Verwendung von Daten für statistische Zwecke, bewährt. Es ist nicht einsichtig, warum in anderen Mitgliedstaaten für derartige Zwecke sensible Daten direkt personenbezogen verwendet werden. Aus dem Verhältnismäßigkeitsgrundsatz ergibt sich, dass solche Daten immer dann verwendet werden sollten, wenn ein direkter Personenbezug nicht notwendig ist (aber andererseits keine völlige

Anonymisierung der Daten möglich ist, etwa, weil ein Krankheitsverlauf bezogen auf spezielle Personen erforscht wird, deren Namen man aber nicht kennen muss).

Es wird vorgeschlagen, das **Konzept der pseudonymisierten Daten** („indirekt personenbezogenen" Daten) in das neue Rechtsinstrument aufzunehmen und für die Verwendung dieser Daten privilegierende Regelungen vorzuschlagen.

Wenn aber eine personenbezogene Verwendung von Daten überhaupt nicht notwendig ist, sollte eine **gänzliche Anonymisierung** der Daten verpflichtend sein.

Zu 2.1.2. *Mehr Transparenz für die von der Verantwortung Betroffenen*

Die Datenschutzkommission begrüßt die Förderung der **Transparenz,** insbesondere im Bereich des Internets, für die Betroffenen und in diesem Zusammenhang den besonderen Schutz von **Minderjährigen.** Auch die Einführung einer generellen „**data breach notification**" wird begrüßt, wobei sich diese Regelung auf schwerwiegende Fälle, in denen etwa den Betroffenen Schaden droht, konzentrieren sollte. Dabei wird auf entsprechende bereits bestehende Regelungen im österreichischen sowie im deutschen Recht hingewiesen.

Zu 2.1.3. *Bessere Kontrolle des Betroffenen über seine Daten*

Die hier genannten Grundsätze werden begrüßt. Es wird darauf hingewiesen, dass es nach österreichischem Recht bereits Fristen für die Gewährung des Auskunfts-, Richtigstellungs- und Löschungsrechts gibt. Auch europaweit wären derartige (harmonisierte) Fristen wünschenswert. Bezüglich der grundsätzlichen Gebührenfreiheit der Ausübung des Auskunftsrechts weist die Datenschutzkommission darauf hin, dass hier ein vernünftiger Ausgleich zwischen den Interessen der Betroffenen und der Auftraggeber zu treffen ist. So hat der Betroffene etwa nach österreichischem Recht die Möglichkeit, einmal im Jahr kostenlos Auskunft aus dem aktuellen Datenbestand zu erhalten. Bei weiteren Anfragen kann ein adäquater Kostenersatz berechnet werden. Weiters wäre auch eine entsprechende Mitwirkungspflicht des Betroffenen zu verankern (siehe z B. § 26 Abs. 3 DSG 2000).

Im Zusammenhang mit dem „*right to be forgotten*" wird angemerkt, dass auch dort, wo Löschungsrechte der Betroffenen bereits nach der Richtlinie 95/46/EG und nach anderen Rechtsinstrumenten existieren, sich das Problem aber hinsichtlich der Durchsetzung in der Praxis stellt, wenn der für die Verarbeitung Verantwortliche der Löschungsverpflichtung nicht nachkommt. Diesbezüglich müssten **effiziente Durchsetzungsmechanismen** geschaffen werden, wobei sich insbesondere die Frage der Durchsetzbarkeit stellt, wenn der für die Verarbeitung Verantwortliche den Sitz in einem Drittstaat hat.

Zu 2.1.4. *Bewusstsein fördern*

Die Datenschutzkommission sieht die Bewusstseinsförderung der Bevölkerung als wesentliche Aufgabe aller mit dem Datenschutz befassten Institutionen an, weist aber darauf hin, dass sich in diesem Zusammenhang wiederum die Frage der zur Verfügung stehenden Ressourcen stellt. Wenn die Datenschutzkontrollbehörden diese Aufgabe ausüben sollen, sollte dies ausdrücklich im neuen Rechtsinstrument verankert werden und bei der Ausstattung berücksichtigt werden.

Zu 2.1.5 *Gewährleistung der Einwilligung ohne Zwang und in Kenntnis der Sachlage*

Die Datenschutzkommission begrüßt eine Harmonisierung bei der Interpretation des Vorliegens einer gültigen Einwilligung.

Zu 2.1.6*. Schutz sensibler Daten*

Es wird eine Erweiterung des Katalogs sensibler Daten auf genetische und biometrische Daten angeregt.

Zu 2.1.7. *Wirksame Rechtsbehelfe und Sanktionen*

Hinsichtlich der Sanktionsmöglichkeiten wird darauf hingewiesen, dass in manchen Mitgliedstaaten die Datenschutzbehörden Strafbefugnisse haben, während in anderen Mitgliedstaaten die Sanktionen von anderen Behörden verhängt werden. Diesbezüglich ist also keine Harmonisierung gegeben, eine solche wäre aber zu begrüßen.

Zu 2.2.2. *Verringerung des Verwaltungsaufwandes*

Die Datenschutzkommission spricht sich für eine Verringerung des Verwaltungsaufwandes aus. In diesem Zusammenhang wird betont, dass durch eine generelle Meldepflicht von Datenanwendungen nicht nur für die „für die Verarbeitung Verantwortlichen“ eine Belastung gegeben ist, sondern vor allem auch für die Datenschutzbehörde selbst; dies zumindest dann, wenn die Datenanwendungen einer rechtlichen Überprüfung unterzogen werden.

Die Datenschutzkommission geht davon aus, dass **„riskante“ Datenanwendungen** (wie etwa jene, die sensible oder strafrechtlich relevante Daten enthalten, die der Beauskunftung der Kreditwürdigkeit einer Person dienen, und dgl.) auch weiterhin einer **Meldung und (Vorab-)Überprüfung** durch die Datenschutzbehörden unterzogen werden sollen. Es wäre zu überlegen, auch bestimmte eingriffsintensive (technische) Verfahren (z.B. die Erstellung von Persönlichkeitsprofilen) einer solchen Überprüfung zu unterwerfen.

Was alle übrigen Meldungen betrifft, so sollte jedoch eine **Entlastung** der Datenschutzkontrollstelle eintreten. Denkbar wäre eine automationsunterstützte Plausibilitätskontrolle oder eine gänzliche Abschaffung derartiger Meldungen. Im letzteren Falle müsste jedoch ein gewisser Ausgleich zur Aufrechterhaltung der Transparenz für die Betroffenen treten (z.B. eine Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten und zur Bereithaltung transparenter Verzeichnisse durch diesen). Dies auch deshalb, weil mangelnde Transparenz ein Ansteigen von Auskunftsbegehren erwarten ließe, was wiederum das Ziel einer Verringerung der Verwaltungslasten konterkarieren würde.

Auf die Ausführungen zu den Punkten 2.2.4. und 2.2.5. wird verwiesen.

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

Die Datenschutzkommission hat im Zusammenhang mit Street View Services festgestellt, dass die Rechtslage für in Österreich aufhältige Personen diesbezüglich unterschiedlich und unbefriedigend ist. Während auf Dienste wie „Google Street View“, das von einem Unternehmen betrieben wird, das seinen Sitz außerhalb der EU hat, österreichisches Recht zur Anwendung kommt, kommen auf andere Dienste, die von auf EU-Gebiet ansässigen Unternehmen betrieben werden, die keine Niederlassung in Österreich haben, Rechtsordnungen anderer EU-Staaten zur Anwendung. Davon abgesehen, dass hier festgestellt wurde, dass die Rechtsordnungen bezüglich dieser Dienste höchst unterschiedlich sind (manche Dienste berufen sich auf das Recht auf freie Meinungsäußerung, was offenbar in manchen Staaten die Anwendung des Datenschutzrechts komplett aushebelt), scheint auch die Rechtsdurchsetzung durch den Betroffenen im Ausland durch faktische Hindernisse (mangelnde Kenntnis der Sprache und Rechtsordnung) schwierig. Es wird angeregt, hier **klare, betroffenenfreundliche und für die Datenschutzbehörden leicht handhabbare Regelungen** zu schaffen.

Zu 2.2.4. *Mehr Verantwortung der für die Verarbeitung Verantwortlichen*

Die Datenschutzkommission geht davon aus, dass in einer Welt, in der die Zahl der einzelnen für die Verarbeitung Verantwortlichen weder überschaubar noch kontrollierbar ist, die **Sicherstellung eines verantwortungsbewussten Umgangs des für die Verarbeitung Verantwortlichen mit personenbezogenen Daten unbedingt notwendig** ist und unterstützt diesen Ansatz der Europäischen Kommission. Zu den „Privacy-by-design“-Projekten siehe auch die Ausführungen zu den „pseudonymisierten Daten“ oben zu Punkt 2.1.1.

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

Die Einführung von EU-Zertifizierungsregelungen wird im Prinzip begrüßt. Sofern diese jedoch zu einer weiteren Belastung der Datenschutzbehörden führen würden, wäre dies ohne zusätzliche Ressourcen nicht möglich.

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

Es wird in Erinnerung gerufen, dass die Regelungen in unterschiedlichen Rechtsinstrumenten im Bereich der ehemaligen ersten und dritten Säule der EU kompetenzrechtliche Gründe hatte, die nunmehr nach Inkrafttreten des Vertrags von Lissabon weggefallen sind. Die Datenschutzkommission spricht sich daher für eine **umfassende und kohärente Datenschutzregelung der EU unter Einbeziehung des Datenschutzes im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** aus; dies natürlich unter Einbeziehung der im Bereich der polizeilichen Arbeit und Strafverfolgung notwendigen Einschränkungen (z.B. im Bereich des Auskunftsrechtes und der Informationsverpflichtung).

Zu 2.4.*Die globale Dimension des Datenschutzes*

Die Datenschutzkommission teilt die Meinung der Europäischen Kommission, dass die derzeitige rechtliche Situation dazu führt, dass der Schutz, der den Betroffenen in einem Drittstaat gewährt wird, von Mitgliedstaat zu Mitgliedstaat unterschiedlich beurteilt werden kann. Dieses Problem wird noch dadurch verschärft, dass im Rahmenbeschluss 2008/977/JI kein der Regelung des Art. 25 Abs. 9 der Richtlinie 95/46/EG vergleichbares Verfahren vorgesehen ist, das Adäquanzentscheidungen der Europäischen Kommission (nach Einholung von Stellungnahmen der Art. 29-Gruppe und des Art. 31-Ausschusses) ermöglicht. Hier scheint eine Harmonisierung geboten.

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

Die Datenschutzkommission unterstützt das Vorhaben einer **Harmonisierung, Stärkung und Präzisierung der Aufgaben der nationalen Datenschutzbehörden**. Die Harmonisierung sollte die Ausgestaltung, Befugnisse und Ausstattung der Datenschutzbehörden betreffen. Letztere sollte sich einerseits an der Bevölkerungszahl des jeweiligen Staates orientieren; andererseits gibt es Aufgaben, die jede Datenschutzkontrollbehörde gleichermaßen trifft (z.B. die Zusammenarbeit mit den anderen Datenschutzbehörden, die Teilnahme und Vor-

und Nachbereitung der Sitzungen der Art. 29-Datenschutz-Gruppe und Untergruppen oder auch Aufgaben wie „Bewusstseinsförderung“ der Bevölkerung etc.), wofür generell eine bestimmte Basisausstattung notwendig ist. Es wird darauf hingewiesen, dass für kleine Datenschutzbehörden derzeit eine Mitarbeit im EU-Bereich und internationalen Bereich in ausreichendem Ausmaß schwer bis gar nicht möglich ist.

Die Datenschutzkommission setzt sich für eine Verbesserung der Zusammenarbeit und Abstimmung zwischen den Datenschutzbehörden ein. In diesem Zusammenhang sollte die Rolle der **Art. 29-Datenschutz-Gruppe gestärkt** werden.

Da die (unabhängige) Art. 29-Datenschutz-Gruppe bislang für Interpretationen der Richtlinie zuständig war, fragt es sich, um welches Verfahren es sich bei dem aus S. 20 der Mitteilung angesprochenen „Verfahren zur Sicherstellung einer einheitlichen Praxis im Binnenmarkt unter der Zuständigkeit der Europäischen Kommission“ handeln soll. Sofern dieses Verfahren Einfluss auf die Arbeit der Art. 29-Gruppe oder deren Unabhängigkeit haben sollte oder die Interpretationen dieser Gruppe außer Kraft setzen würde, wäre ein derartiges Verfahren abzulehnen.

Die Datenschutzkommission ersucht, diese Stellungnahme bei Erstellung des Entwurfes eines Datenschutzrechtsinstruments zu berücksichtigen.

17. Dezember 2010
Für die Datenschutzkommission
Der Vorsitzende:
Senatspräsident des OGH Dr. SPENLING

Für die Richtigkeit
der Ausfertigung: