REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.352/0004-DSR/2009
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für Justiz

An das
Bundesministerium für Inneres

Betrifft: Mitteilung der Kommission vom 10.6.2009 KOM (2009) 262 endg. („Stockholm Programm“)

Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner 189. Sitzung am 3. Juli 2009 **einstimmig beschlossen**, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

Der **Datenschutzrat weist darauf hin**, dass **rechtzeitig** die Stellungnahmen des **Bundesministeriums für Inneres** und des **Bundesministeriums für Justiz an den Datenschutzrat übermittelt werden sollen**, damit der Datenschutzrat in den Meinungsbildungsprozess eingebunden wird und noch vor Abschluss der Willensbildung im Bereich der Exekutive Stellung nehmen kann.

I. Allgemeines

Eine wesentliche, primärrechtlich verankerte Zielvorgabe (vgl. Art. 61 EG-Vertrag, Art. 2 Abs. 1, 4. Spiegelstrich und Art. 29 Abs. 1 EUV) der EU besteht in der Etablierung eines „Raumes der Freiheit, der Sicherheit und des Rechts“. Zur Erreichung dieses Zieles sollen mehrjährige „Rahmenprogramme“ beitragen, mit

denen eine entsprechende Konkretisierung erfolgt. Das aktuell maßgebliche Programm, das sog. „Haager Programm“ (2005 bis 2010) soll nunmehr durch ein daran anschließendes abgelöst werden. Hiezu gibt es bereits einschlägige, im Rahmen des Rates entwickelte Vorschläge.

Nunmehr hat auch die Kommission in Form ihrer „Mitteilung an das Europäische Parlament und den Rat: Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger“ vom 10. Juni 2009 (KOM [2009] 262 endg.) ihre Vorstellungen präsentiert.

II. Zu den Inhalten der Kommissionsmitteilung KOM [2009] 262

A. Grund- und Bürgerrechtspolitik

1. Ausgewählte Positionen der Kommission

Begrüßenswert erscheint der grundlegende Ansatz der Kommission („Leitmotiv“), der darin bestehen soll, mit dem neuen Programm ein „Europas der Bürger“ aufzubauen. „Alle Maßnahmen sollen den Bürger in den Mittelpunkt stellen […]“ (vgl. KOM [2009] 262 endg., S. 5). Der Raum der Freiheit, der Sicherheit und des Rechts soll vor allem ein gemeinsamer Raum des Grundrechtsschutzes sein, in dem der Respekt der menschlichen Person und ihrer Würde sowie der übrigen in der Grundrechte-Charta verankerten Rechte im Mittelpunkt steht. Dazu zählen die Wahrung der persönlichen Freiheitsrechte und der Privatsphäre über Staatsgrenzen hinweg, z.B. durch Datenschutz […]. und die uneingeschränkte Ausübung der individuellen Rechte auch in Drittländern (vgl. KOM [2009] 262 endg., S. 5 f).

Zugleich soll zufolge der Kommission „eine Strategie für die innere Sicherheit entwickelt werden, um die Sicherheitslage innerhalb der Union zu verbessern und damit das Leben und die Unversehrtheit der europäischen Bürger zu schützen“. Die Strategie sollte die Intensivierung der Zusammenarbeit der Polizei- und Justizorgane sowie bessere Sicherheitsvorkehrungen bei der Einreise in die EU bezwecken (vgl. KOM [2009] 262 endg., S. 6).

Weiters erinnert die Kommission daran, dass Infolge des Inkrafttretens des Vertrages von Lissabon der Beitritt der Union zur Europäischen Menschenrechtskonvention in

Aussicht genommen ist (vgl. Art 6 Abs 2 EUV i.d.F. Vertrag von Lissabon), womit ein „politisches Signal“ gesetzt werden solle (vgl. KOM [2009] 262 endg. S. 7).

Hervorgehoben wird weiters insbesondere die Bedeutung der Fortsetzung des Kampfs gegen Diskriminierung, Rassismus, Antisemitismus, Fremdenfeindlichkeit und Homophobie, das Erfordernis, sich mit vereinten Kräften für eine vollständige Eingliederung von schutzbedürftigen Bevölkerungsgruppen und speziell der Roma in die Gesellschaft einzusetzen, indem deren Einbindung in das Schulsystem und den Arbeitsmarkt gefördert wird und etwaige gegen diese gerichtete Gewaltakte unterbunden werden (vgl. KOM [2009] 262 endg., S. 8).

Bemerkenswert ist, dass die Kommission dem „Schutz personenbezogener Daten und Schutz der Privatsphäre“ einen eigenen Abschnitt im Rahmen ihrer Grundrechtspolitischen Erwägungen widmet (vgl. KOM [2009] 262 endg. S. 9).

Die Union müsse „neue allumfassende Maßnahmen zum Schutz der Daten der Bürger innerhalb der Europäischen Union und im Verhältnis zu Drittstaaten ergreifen“. Sie müsse auch klären, unter welchen Umständen Behörden in Ausübung ihrer rechtmäßigen Funktionen der Anwendung dieser Vorschriften gegebenenfalls Grenzen setzen könnten.

Der derzeitige rechtliche Rahmen gewährleiste ein hohes Schutzniveau, jedoch bedürfe es in Anbetracht des raschen technologischen Wandels zusätzlicher Maßnahmen – ob legislativer oder sonstiger Art sei fürs Erste dahingestellt – um diese Grundsätze aufrechtzuerhalten.

Daneben müssten geeignete neue Technologien entwickelt werden, die den Anforderungen an den Datenschutz Rechnung tragen. Zu diesem Zweck müsse die Zusammenarbeit zwischen öffentlichem und privatem Sektor speziell im Bereich der Forschung verbessert werden. „Datenschutzfreundliche“ Technologien, Produkte und Dienstleistungen sollten eventuell mit einem europäischen Prüfsiegel versehen werden.

Ein wirksamer Datenschutz setze nicht zuletzt eine gute Kenntnis der Rechte und der Gefahren (vor allem des Internets) voraus, weshalb Informations- und Aufklärungskampagnen geplant seien, die sich insbesondere an die am stärksten gefährdeten Personengruppen richten.

Alles in allem bestehe die Aufgabe der Union darin, bei der Entwicklung und Förderung internationaler Standards im Bereich des Schutzes personenbezogener Daten und beim Abschluss geeigneter internationaler Instrumente auf bi- oder multilateraler Ebene als treibende Kraft zu wirken. Die Zusammenarbeit mit den Vereinigten Staaten auf dem Gebiet des Datenschutzes könnte als Vorbild für weitere Abkommen dieser Art dienen.

Erwähnenswert erscheint weiters, dass die Kommission mit Blick auf die Europawahlen 2014 anregt, Überlegungen anzustellen, wie mehr Bürger an die Wahlurnen gebracht werden können: angestrebt werden sollten u.a. „Erleichterungen bei allen Wahlvorgängen, bei der Eintragung in das Wählerverzeichnis oder die Festsetzung eines gemeinsamen Wahltermins“ […] (vgl. KOM [2009] 262 endg, S. 10).

2. Bewertung

Uneingeschränkt positiv zu bewerten sind die zahlreichen Bekenntnisse der Kommission zum Grundrechtsschutz im Allgemeinen und zum Grundrecht auf Datenschutz bzw. zum Menschenrecht auf Privatsphäre im Besonderen. Analoges gilt für die Erkenntnis des Erfordernisses zusätzlicher Schutzmaßnahmen im Lichte des technologischen Wandels, aber auch für den Hinweis auf die Notwendigkeit von internationalen, über die EU hinausreichenden Datenschutz-Standards.

Die legistische und politische Praxis der Kommission in der jüngeren Vergangenheit freilich steht mehrfach in einem auffallenden Spannungsverhältnis zu den vorstehend skizzierten Postulaten. Gerade in Bezug auf die ständig steigenden Begehrlichkeiten etwa der Vereinigten Staaten nach Zugriffen auf Daten von EU-Bürgern (Stichworte: „SWIFT-Affäre“, Flugpassagierdaten, u.v.m.) ist es der Kommission bis dato gerade nicht gelungen, durch verhältnismäßige Lösungen und ausreichende Individualrechtsschutzmechanismen dem europäischen Rechtsrahmen sowie den nationalen Verfassungstradtionen auf dem Felde der Grund- und Menschenrechte genügend Rechnung zu tragen.

Zum Thema „neue Datenschutztechnologien“ ist anzumerken, dass die Problematik zunächst weniger im Fehlen von „datenschutzfreundlichen“ Technologien zu sehen ist, als in rechtlichen /politischen Zielvorgaben für die IT-Industrie bzw. die

Dienstleistungswirtschaft i.w.S. So wäre es dringend geboten, auf europäischer Ebene bspw. den Grundsatz zu verankern, 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.

Zu den von der Kommission angesprochenen „Erleichterungen" bei allen Wahlvorgängen zwecks Hebung der Wahlbeteiligung ist anzumerken, dass unklar bleibt, in welche Richtung solche Erleichterungen gehen sollen. Insbesondere ist fraglich, ob die Kommission bspw. an eine Stimmabgabe via Internet denkt. Letzteres hätte wiederum Relevanz insbesondere für das Grundrecht auf Datenschutz. Da die Ausgestaltung des konkreten Wahlmodus für EU-Parlamentswahlen derzeit in die nationale Kompetenz fällt, scheint ein näherer Diskussionsbedarf momentan freilich nicht gegeben.

B. Verstärkung der grenzüberschreitenden behördlichen Zusammenarbeit iwS

1. Ausgewählte Vorschläge der Kommission

Im Kontext der „weiteren Umsetzung des Grundsatzes der gegenseitigen Anerkennung" weist die Kommission insbesondere darauf hin, dass künftig bestimmte Geldbußen, die je nach Mitgliedstaat straf- oder verwaltungsrechtlicher Natur sind, in anderen Mitgliedstaaten vollstreckt werden können müssen, z. B. wenn sie der Sicherheit im Straßenverkehr oder ganz allgemein der Durchsetzung der EU-Politik dienen.

Mit Blick auf die besagte gegenseitige Anerkennung von Entscheidungen, die Rechtsverluste zum Gegenstand haben, müsse die EU den systematischen Informationsaustausch zwischen den Mitgliedstaaten fördern (vgl. KOM [2009] 262 endg., S. 10).

Unter der „Rubrik" „E-Justiz" stellt die Kommission u.a. fest, dass vorgesehen ist, „auch im Einklang mit den Datenschutzbestimmungen" die schrittweise Vernetzung einer Reihe von nationalen Registern (z. B. Insolvenzregister natürlicher und juristischer Personen) vorzunehmen (vgl. KOM [2009] 262 endg., S. 14).

Ausdrücklich angesprochen wird die Thematik der Vernetzung von nationalen Registern zudem im Kontext der „inneren Sicherheit“ (Stichwort: „Europäisches Strafregisterinformationssystem – ECRIS“; dazu noch weiter unten) (vgl. KOM [2009] 262 endg.; S. 19).

2. Bewertung

Es fällt auf, dass die vorstehend skizzierte Verstärkung der Behördenzusammenarbeit unter der Überschrift „Erleichterungen für die Bürger“ erfolgt (vgl. KOM [2009] 262 endg., S. 10). Damit soll möglicherweise der Eindruck erweckt werden, die nachfolgend diskutierten Maßnahmen kämen primär den Bürgen zugute. Tatsächlich geht es dabei insbesondere auch um Maßnahmen, die auf eine grenzüberschreitende Verfolgung von Verwaltungsübertretungen (Falschparken, Geschwindigkeitsübertretungen) abzielen, verbunden mit Rechtsfolgen für die Betroffenen bis hin zu Rechtsverlusten (Berufsverbote, Führerscheinentzug).

Der damit verbundene verstärkte grenzüberschreitende Austausch von personenbezogenen Daten wirft zahlreiche grundrechtliche Fragestellungen auf, die (mit)geregelt bzw. mitbedacht werden müss(t)en (Bsp: Einziehen von Schwellen, um Bagatelldelikte auszuschließen; Klare Regeln betreffend Speicherdauer bzw. Löschung von Verwaltungsstrafdaten; Regelung/Beschränkung des grenzüberschreitenden Zugriffs auf „Vorstrafen“ etc.).

Ebenfalls als „Vorteil eines europäischen Rechtsraums“ für die Bürger weist die Kommission das Vorhaben einer Vernetzung diverser nationaler Justizregister aus. Die datenschutzrechtlichen Fragen, die sich hier stellen, sind wiederum als überaus komplex zu bezeichnen. Sollen bspw. national bestehende Löschungspflichten oder Auskunfts- bzw. Übermittlungsbeschränkungen nicht unterlaufen werden, bedarf es eines grundsätzlichen restriktiven bzw. umsichtigen Ansatzes unter besonderer Berücksichtigung der Transparenz für die Betroffenen.

C. Innere Sicherheit (ausgewählte Aspekte)

1. „Informationsmanagement“, „Informationstechnologie“, polizeiliche Zusammenarbeit

a) Überlegungen der Kommission

Im Kontext der inneren Sicherheit spricht die Kommission u.a. davon, dass es gelte, eine gemeinsame Sicherheitskultur zu haben, den Informationsaustausch zu optimieren und auf eine angemessene technische Infrastruktur zurückgreifen zu können. Für die Sicherheit der EU bedürfe es leistungsfähiger Systeme für den Informationsaustausch zwischen den nationalen Behörden und den europäischen Stellen. Die EU brauche daher ein europäisches Informationsmodell mit einer verstärkten strategischen Analysekapazität und gleichzeitig einer besseren Erfassung und Verarbeitung operativer Informationen. Dieses Modell müsse die bestehenden Strukturen, einschließlich der Zollbehörden, berücksichtigen und auch den Schwierigkeiten des Informationsaustauschs mit Drittstaaten gerecht werden (vgl. KOM [2009] 262 endg., S. 16). Wichtig sei es hiebei, insbesondere die Grundlinien einer Politik für den grenzüberschreitenden Informationsaustausch im Zusammenhang mit Sicherheitsmaßnahmen „unter Beachtung der strengen Datenschutzanforderungen“ festzulegen.

[…] Die neuen Technologien müssten „mit den Entwicklungen der Mobilität mitziehen und diese unterstützen“, gleichzeitig aber auch die Sicherheit und Freiheit des Einzelnen gewährleisten helfen. Forschung und Entwicklung im Bereich der Sicherheit müssten mit den Schwerpunkten der Strategie der inneren Sicherheit abgestimmt sein und sich auf die Verbesserung der Interoperabilität, die Ermittlung des Bedarfs und der in Frage kommenden Technologien, die Validierung der Ergebnisse und die Entwicklung geeigneter Standards konzentrieren. Die Forschungsanstrengungen müssen auf die tatsächlichen Bedürfnisse der Benutzer ausgerichtet sein und müssen von öffentlich-privaten Partnerschaften unterstützt werden […] (vgl. KOM [2009] 262 endg., S. 17).

Es gelte im Übrigen, das Potenzial von Europol besser zu nutzen; die Behörde müsse systematisch über den Einsatz von gemeinsamen Untersuchungsteams informiert werden und in wichtige grenzüberschreitende Operationen einbezogen

werden. Wenn klar ist, welche Arten von Daten auszutauschen sind, müssten Verfahren für die automatische Datenübertragung an Europol eingerichtet werden. Europol müsse zudem seine Verbindungen zu Eurojust ausbauen, damit die gerichtliche Weiterverfolgung der Fälle, mit denen es befasst ist, gewährleistet ist.

b) Bewertung

Anzumerken ist, dass die Ausführungen zum Thema „Informationstechnologie“ vage bleiben. Wenn im Kontext der sog. „3. Säule“ der EU auf „die strengen Datenschutzanforderungen Bezug genommen wird, bleibt nur festzustellen, dass es auf europäischer Ebene keine ebensolchen gibt oder solche nur lückenhaft und punktuell in einzelnen Rechtsakten verankert sind. Der Rahmenbeschluss für die 3. Säule bedeutet bekanntlich gerade keine Harmonisierung der nationalen Datenschutzniveaus.

Skepsis geboten ist zudem stets, wenn im gegebenen Kontext von einer „Verbesserung der Interoperabilität“ die Rede ist. Der Terminus ist insofern potentiell irreführend, als sich dahinter die Idee einer weitgehenden Vernetzung von Datenanwendungen verbirgt, mit dem Ziel, diese leicht miteinander abgleichbar zu machen, oder anhand eines zentralen Personenkennzeichens (biometrisches Merkmal „Fingerabdruck“ u.a.) fix zu verknüpfen. Ein solcher, auch aus den Ratsdokumenten zum Stockholmer Programm hervorgehender Ansatz steht freilich dem datenschutzrechtlichen Grundsatz der Zweckbindung fundamental entgegen.

2. „Strafjustiz zum Schutz der Bürger“

a) Überlegungen der Kommission

Die EU brauche, so die Kommission, ein umfassendes System für die Beweiserhebung in grenzüberschreitenden Angelegenheiten. Dies müsse auch eine Europäische Beweisanordnung umfassen, die alle bisherigen rechtlichen Instrumente ersetzt. Diese Anordnung, die in der gesamten EU automatisch anerkannt werde und Gültigkeit habe, werde eine flexible und effiziente Zusammenarbeit zwischen den Mitgliedstaaten fördern. Sie werde feste Ausführungsfristen vorsehen, eine Ablehnung wird nur in ganz begrenzten Fällen möglich sein. Zu prüfen sei außerdem:

– eine europäische Regelung für die Zulassung elektronischer Belege,

– ein europäisches System für Anweisungen, Personen zwangsweise vorzuführen, unter Berücksichtigung der Videokonferenzmöglichkeiten, sowie

– Mindeststandards für die gegenseitige Anerkennung von Beweismitteln unter den Mitgliedstaaten, darunter auch wissenschaftlicher Beweise (vgl. KOM [2009] 262 endg., S. 19).

Zudem müsse der Aufbau des Europäischen Strafregisterinformationssystems (ECRIS) weiter vorangetrieben werden, wobei der Informationsaustausch einer Bewertung zu unterziehen sei. Durch die Vernetzung der einzelstaatlichen Strafregister sollten bestimmte Straftaten verhindert werden können (beispielsweise im Zusammenhang mit bestimmten Berufstätigkeiten, vor allem in der Kinderbetreuung). Außerdem sollten auch in der EU verurteilte Drittstaatsangehörige im ECRIS erfasst werden.

b) Bewertung

Zur Thematik einer künftigen, weiterentwickelten europäischen Beweisanordnung ist anzumerken, dass sich als Konsequenz eine Aushöhlung nationaler Verfahrensvorschriften ergeben könnte, die in der Bindung an richterliche Genehmigungen bestehen (Stichwort: Fernmeldegeheimnis u.ä.). Müssen ausländische Beweisanordnungen in Österreich anerkannt werden, die auf Zwangsmaßnahmen hinauslaufen (Telefonabhörung, Datenbeschlagnahme etc.), und besteht im Ausland bspw. eine entsprechende Anordnungsbefugnis auch für die dortige Polizeibehörde ohne Mitwirkung der Gerichte (wie bspw. in Großbritannien), so könnten im Ergebnis die nationalen (noch) bestehenden Kontrollvorkehrungen durch Gerichte ins Leere laufen.

Zur Problematik der Vernetzung von Justizregistern sei einmal auf die Erwägungen oben in Abschnitt B.2 verwiesen. Zudem sei angemerkt, dass eine grenzüberschreitende Vernetzung der Strafregister möglicherweise dazu führt, dass infolge national unterschiedlicher Zugriffsbefugnisse und Weiterverwendungsregelungen erhebliche datenschutzrechtliche Defizite auftreten. Mit der bloßen wechselseitigen Öffnung der Register ist es somit nicht getan. Es bedürfte eines europaweit einheitlichen Datenverwendungsstandards.

3. „Außengrenzkontrolle“

a) Überlegungen der Kommission

Unter der Rubrik „Kontrolle und Überwachung der Grenzen“ betont die Kommission, dass ein „integriertes Grenzmanagement“ erforderlich sei. Dies setzte die weitere Modernisierung des Schengen-Besitzstands und den Ausbau der Kooperationen voraus […]. Ein hohes Maß an innerer Sicherheit müsse mit der uneingeschränkten Achtung der Menschenrechte und der Garantie von internationalem Schutz Hand in Hand gehen (vgl. KOM [2009] 262 endg., S. 20).

[…] Die Kontrollen (Sicherheits-, Einwanderungs-, Zollkontrollen) an den Grenzübergängen müssten vor allem durch die Trennung von Privat - und Geschäftsreisenden an den Kontrollstellen rationalisiert werden. In bestimmten Fällen seien dazu bauliche Veränderungen an den bestehenden Grenzübergängen und der verstärkte Einsatz neuer Technologien (biometrische Identifikatoren u.s.w.) nötig. Durch eine engere Zusammenarbeit zwischen den nationalen Behörden würden die Verfahren vereinfacht, wodurch die Unannehmlichkeiten beim Überschreiten der Grenzen verringert werden. Auch können dadurch die Ressourcen optimal eingesetzt werden (vgl. KOM [2009] 262 endg., S. 20).

Vorgesehen seien weiters ein elektronisches Registriersystem für Ein und Ausreisen in die bzw. aus den Hoheitsgebieten der EU-Mitgliedstaaten sowie Programme für registrierte Reisende (RTP). Eine neue Agentur könnte diese Systeme, die 2015 operationell sein sollen, entwickeln. Die EU wird auch über die mögliche Einführung eines europäischen Vorabgenehmigungssystems für Reisen entscheiden.

b) Bewertung

Der von der Kommission auf dem Felde der Außengrenzkontrollen verfolgte Ansatz wirft nicht nur schwerwiegende datenschutzrechtliche, sondern auch darüber hinausreichende Probleme auf. So könnte die Bildung von Gruppen von Einreisenden („Geschäftsreisende“ versus „normale Bürger“) mit dem Gleichheitsgrundsatz konfligieren bzw. zu Diskriminierungen führen.

Zu den Plänen einer „biometrie-gestützten“, automatisiert ablaufenden Kontrolle an der Grenze in Form einer „Selbstabfertigung“ ist anzumerken, dass tatsächliche Effizienzgewinne erst dargelegt werden müssten. Technologiebedingt (fehlerhafte Zurückweisung etc.) kommen biometrie-gestützte Identifizierungssystem wahrscheinlich nicht ohne zusätzliche Personalressourcen an der Grenze aus (für manuelle Eingriffe bei „Zurückweisungen“ und automatisierten „Treffermeldungen“ b.z.w. bei detaillierter Überprüfung der Betroffenen).

Aus datenschutzrechtlicher Sicht ist wiederum auf die Unverhältnismäßigkeit einer solchen Maßnahme (Erhebung zusätzlicher Daten von den Betroffenen) bzw. die signifikant erhöhte staatliche Kontrolldichte („Reiseprofile“ etc.) zu verweisen.

15. Juli 2009
Für den Datenschutzrat:
Der Vorsitzende:
WÖGERBAUER

Elektronisch gefertigt