PETER HUSTINX
DATENSCHUTZBEAUFTRAGTER

An den Präsidenten des Rates der
Europäischen Union
Generalsekretariat
Rat der Europäischen Union
Rue de la Loi 175
1048 Brüssel

Brüssel, 14. Februar 2014
PH/ABu/mk/ D(2014)0375 **C2011-1104**

Betrifft: Fortschritte beim Datenschutzreformpaket

Sehr geehrter Herr Präsident,

mit Blick auf die laufenden Verhandlungen über das Datenschutzreformpaket und insbesondere auf die anstehende Tagung des JI-Rates am 3./4. März möchten wir Sie auf eine Reihe noch offener Fragen hinweisen.

Die Modernisierung des bestehenden EU-Regelwerks für den Schutz personenbezogener Daten ist erforderlich, damit der EU-Gesetzgeber seinen Verpflichtungen nach Artikel 16 AEUV nachkommt. Sie ist ferner von wesentlicher Bedeutung für einen wirksamen Schutz der Grundrechte der EU-Bürger auf den Schutz der Privatsphäre und den Schutz ihrer personenbezogenen Daten, wie er in Artikel 7 und 8 der Charta der Grundrechte der EU verankert ist[1].

Unserer Auffassung nach bedürfen die Datenschutzvorschriften der EU dringend einer Reform, damit in der EU insgesamt der Datenschutz kohärenter und einheitlicher gestaltet wird und somit gleiche Bedingungen für Online- wie für traditionelle Marktteilnehmer geschaffen werden. Die Bürger wiederum verdienen einen wirksameren Schutz ihrer Grundrechte auf Schutz der Privatsphäre und Schutz personenbezogener Daten, der nur geboten werden kann, wenn der geltende Rechtsrahmen in sich schlüssig ist (also eine möglichst breite Palette Daten verarbeitender Stellen und Tätigkeiten abdeckt) und möglichst

[1] Siehe unter anderem die Stellungnahme des EDSB zum Datenschutzreformpaket vom 7. März 2012.

kohärent ist (also in den 28 Mitgliedstaaten so einheitlich angewandt wird, wie dies in der Praxis erreichbar ist).

Wir begrüßen die derzeitigen Bemühungen des griechischen Ratsvorsitzes um Fortschritte in einer Reihe offener Fragen. Ferner begrüßen und unterstützen wir die Zielsetzung, eine Einigung über ein Mandat für die Verhandlungen mit dem Europäischen Parlament bis zum Ende des griechischen Ratsvorsitzes zu erzielen und den Verhandlungsprozess bis Ende 2014 abzuschließen.

Bei einer ganzen Reihe wichtiger Bestandteile des Datenschutzpakets steht jedoch fest, dass Kompromisslösungen noch nicht in Sicht sind. Noch beunruhigender ist jedoch, dass der bestehende *acquis* in mancherlei Hinsicht geschwächt werden könnte (beispielsweise beim Anwendungsbereich der vorgeschlagenen Datenschutz-Grundverordnung).

In Anbetracht der derzeit stattfindenden Diskussionen halten wir es für sinnvoll, die Haltung des EDSB zu drei zentralen, noch offenen Fragen im Zusammenhang mit der vorgeschlagenen Datenschutz-Grundverordnung noch einmal darzulegen. Wir betrachten dies als wesentlichen Aspekt unserer Rolle als Berater der EU-Organe in allen Fragen des Schutzes personenbezogener Daten.

1. Anwendungsbereich der vorgeschlagenen Datenschutz-Grundverordnung

Soweit wir wissen, ist die Option einer Ausnahme des öffentlichen Sektors vom Anwendungsbereich der Datenschutz-Grundverordnung – oder zumindest der Einführung weitreichender Ausnahmen und Befreiungen – noch nicht vom Tisch. Diesbezüglich sei uns der Hinweis gestattet, dass weder in der derzeit geltenden Datenschutzrichtlinie 95/46/EG noch im Übereinkommen Nr. 108 des Europarates (zu dessen Vertragsparteien alle Mitgliedstaaten gehören) zwischen „privatem“ und „öffentlichem“ Sektor unterschieden wird.

Ein Ausschluss des öffentlichen Sektors würde also nicht nur den Gesetzgebungsprozess erheblich verzögern, sondern würde, bezogen auf das heutige Datenschutzregelwerk, auch einen deutlichen Rückschritt bedeuten. Darüber hinaus dürften ein Ausschluss des öffentlichen Sektors oder weitreichende Ausnahmen kaum gerechtfertigt oder erforderlich sein. Schon heute sehen die geltenden Datenschutzvorschriften für öffentliche Einrichtungen umfangreiche Möglichkeiten der Verarbeitung personenbezogener Daten vor, sofern diese erforderlich ist, um einer rechtlichen Verpflichtung nachzukommen, oder zur Wahrnehmung von Aufgaben im öffentlichen Interesse, und daran wird sich auch mit der vorgeschlagenen Datenschutz-Grundverordnung nichts ändern.

Weiter ist die Grenze zwischen dem „öffentlichen“ und dem „privaten“ Sektor weniger eindeutig, als es vielleicht aussieht. So kann beispielsweise die gleiche Art von Tätigkeit (z. B. Erbringung von Gesundheitsdiensten) in einem Mitgliedstaat durch private Einrichtungen, in einem anderen Mitgliedstaat durch öffentliche Einrichtungen oder innerhalb ein- und desselben Mitgliedstaats sowohl von privaten als auch von öffentlichen Einrichtungen erbracht werden. **Sehr ähnliche Einrichtungen**, die die gleichen Kategorien personenbezogener Daten verarbeiten (wie Krankenhäuser oder Universitäten) **sollten unabhängig davon, ob sie in Privatbesitz oder im Besitz des Staates sind, dem gleichen Regelwerk unterstehen**.

Und ein Datenaustausch zwischen öffentlichen Stellen und privaten Einrichtungen, der die Lebensader einer modernen Wirtschaft ist und jeden Tag im Rahmen von Auslagerungen oder

öffentlich-privaten Partnerschaften erfolgt, kann reibungslos nur erfolgen, wenn überall die gleichen Regeln gelten. Häufig sind öffentliche Einrichtungen am Markt tätig. Würden für sie andere Datenschutzvorschriften als für private Marktteilnehmer gelten, hätte dies unvermeidlich Wettbewerbsverzerrungen im Binnenmarkt zur Folge.

Schließlich würde ein solches massives Abweichen vom EU-Regelwerk für den Schutz personenbezogener Daten die Verhandlungsposition der EU in ihren Verhandlungen mit Drittländern schwächen, insbesondere in den Fällen, in denen die EU auf die Annahme eines umfassenden Datenschutzrechtsrahmens gedrängt hat. Gleiches würde eintreten, wenn für den öffentlichen Sektor weitreichende Ausnahmen vorgesehen würden, es sei denn, diese wären unbedingt erforderlich und blieben auf ganz konkrete Situationen beschränkt, die durch die bestehenden Ausnahmen nicht abgedeckt sind.

2. Grundsatz der zentralen Anlaufstelle

In einfachen Worten bedeutet der Grundsatz der zentralen Anlaufstelle, dass in Fällen, in denen die Verarbeitung personenbezogener Daten in mehr als einem Mitgliedstaat stattfindet, eine einzige Aufsichtsbehörde für die Überwachung der Tätigkeit des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters in der gesamten Union zuständig ist und die entsprechenden Beschlüsse fasst. Laut Vorschlag wäre dies im Regelfall die Aufsichtsbehörde des Mitgliedstaats, in dem die Daten verarbeitende Stelle ihre „Hauptniederlassung" hat; diese Behörde würde als „Aufsicht führende Behörde" bezeichnet. Unserer Auffassung nach sollte die Rolle einer Aufsicht führenden Behörde nicht als ausschließliche Zuständigkeit verstanden werden, sondern vielmehr als eine strukturierte Zusammenarbeit mit anderen, örtlich zuständigen Aufsichtsbehörden. Die Aufsicht führende Behörde würde nämlich in hohem Maße von Beiträgen und der Unterstützung der anderen Aufsichtsbehörden in allen Phasen des Prozesses abhängen[2].

Der Grundsatz der zentralen Anlaufstelle ist ein wichtiges Element der vorgeschlagenen Harmonisierung des Datenschutzregelwerks. Er wurde von der Kommission ins Spiel gebracht, um die einheitliche Anwendung der Vorschriften zu verbessern, Rechtssicherheit zu gewährleisten und den Verwaltungsaufwand der für die Verarbeitung Verantwortlichen und Auftragsverarbeiter zu verringern, die in mehr als einem Mitgliedstaat tätig sind.[3] Er verringert die Fragmentierung der Datenschutzlandschaft. Für Unternehmen ist es wichtig, mit (im Idealfall) einem Gesprächspartner und nicht mit (möglicherweise) 28 nationalen Aufsichtsbehörden zu tun zu haben. Wir weisen darauf hin, dass der JI-Rat den Grundsatz im Oktober 2013 gebilligt und ihn zusammen mit dem Kohärenzverfahren als „eine der tragenden Säulen des Kommissionsvorschlags" bezeichnet hat.

Im vergangenen Dezember erhob der Juristische Dienst des Rates eine Reihe rechtlicher Einwände gegen den Grundsatz der zentralen Anlaufstelle und stellte dabei dessen Vereinbarkeit mit der Charta der Grundrechte der EU in Frage, insbesondere mit Artikel 47 der Charta, der das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht vorsieht und inhaltlich Artikel 13 und Artikel 6 Absatz 1 EMRK entspricht. Die größten Bedenken scheinen bezüglich der „Nähe" zwischen der Aufsichtsbehörde, die in einem konkreten Fall einen Beschluss fasst, und dem einzelnen Bürger zu bestehen, die als „ein wichtiger Aspekt des Schutzes der Rechte des Einzelnen" angesehen wurde.

[2] Siehe Stellungnahme des EDSB vom 7. März 2012, Punkt 237.
[3] Erwägungsgrund 97 des Kommissionsvorschlags.

Unserer Auffassung nach malt der Juristische Dienst des Rates mit seiner Auslegung des Grundsatzes der zentralen Anlaufstelle ein **übermäßig negatives Bild** der derzeit erörterten Vorschläge. Aus unserer Sicht ist es durchaus möglich, den Grundsatz mit einem hohen Schutzniveau für die Grundrechte der Bürger einschließlich der durch Artikel 47 der Charta geschützten zu vereinbaren. Unsere Auffassung stützt sich auf eine Reihe von Erwägungen, von denen wir Ihnen die wichtigsten kurz darstellen möchten.

Zu allererst sei drauf hingewiesen, dass gemäß Artikel 28 Absatz 6 der Richtlinie 95/46/EG eine Kontrollstelle im Hoheitsgebiet ihres Mitgliedstaats immer für die Ausübung ihrer Befugnisse zuständig ist (die auch die Untersuchung von Beschwerden umfassen). Sofern es sich nicht um eine Beschwerde über einen für die Verarbeitung Verantwortlichen (oder einen Auftragsverarbeiter) mit einer Niederlassung oder Ausrüstung in dem betreffenden Mitgliedstaat handelt[4], können die tatsächlichen Befugnisse dieser Kontrollstelle in der Praxis durchaus beschränkt sein. Die Notwendigkeit nämlich, in einem konkreten Fall das einzelstaatliche Recht eines anderen Mitgliedstaats anzuwenden, sowie fehlende Möglichkeiten zur Durchführung von Untersuchungen oder zur Verhängung von Sanktionen, wenn der für die Verarbeitung Verantwortliche/Auftragsverarbeiter physisch nicht präsent ist, kann das Anrufen der Kontrollstelle zu einer rein theoretischen und weitgehend unwirksamen Lösung machen.

Die vorgeschlagene Datenschutz-Grundverordnung würde hingegen einen einheitlichen rechtlichen Rahmen gewährleisten und Mechanismen für eine wirksame Durchsetzung durch Aufsichtsbehörden in der Praxis vorsehen. Zunächst einmal hätten alle Bürger zur Ausübung ihrer Rechte ausdrücklich das Recht auf Beschwerde bei der örtlichen Aufsichtsbehörde (oder auch einer anderen Aufsichtsbehörde)[5]. Wichtiger ist aber, dass in Fällen, in denen heute eine Aufsichtsbehörde nur über begrenzte Möglichkeiten verfügen würde, die neue Verordnung für eine wirksame Durchsetzung durch die Aufsicht führende Behörde im Rahmen der zentralen Anlaufstelle (durch Nutzung der Vorteile des Kohärenzverfahrens[6]) sorgen könnte, bei Bedarf mit Unterstützung durch die örtlich zuständige Aufsichtsbehörde. Darüber hinaus hat jede natürliche Person immer das Recht, gegen ein in ihrem Land niedergelassenes Unternehmen vor den Gerichten dieses Landes wegen eines mutmaßlichen Verstoßes gegen die Verordnung Klage zu erheben[7].

Aus diesem Blickwinkel wird sich die vorgeschlagene Datenschutz-Grundverordnung **äußerst positiv** auf die Möglichkeiten natürlicher Personen **auswirken**, ihre Datenschutzrechte durchzusetzen; somit würde sie den Schutz des Rechts auf wirksamen Rechtsbehelf, wie er in Artikel 47 der Charta verankert ist, **deutlich verbessern**.

Die vorgeschlagene Datenschutz-Grundverordnung sieht ferner eine Überprüfung von Entscheidungen von Aufsichtsbehörden durch die Gerichte vor[8]. In Fällen, in denen der Grundsatz der zentralen Anlaufstelle gilt, müsste eine natürliche Person, die eine Entscheidung der Aufsicht führenden Aufsichtsbehörde anfechten möchte, dies vor einem Gericht in dem Mitgliedstaat der Aufsicht führenden Behörde tun; in vielen Fällen würde dies in der Praxis bedeuten, dass Klage in einem anderen Mitgliedstaat erhoben wird.

[4] Dies ergibt sich aus den Bestimmungen über das anwendbare Recht in Artikel 4 Absatz 1 Buchstabe a, b und c.
[5] Artikel 73 Absatz 1 des Vorschlags.
[6] Kapitel VII des Vorschlags.
[7] Artikel 75 des Vorschlags.
[8] Artikel 73 des Vorschlags.

In diesem Zusammenhang sind wir der Auffassung, dass allein die Tatsache, dass Gerichte in einem anderen Mitgliedstaat als dem Wohnsitzmitgliedstaat eines Bürgers angerufen werden müssen, diesen nicht eines wirksamen Rechtsschutzes beraubt. Nach der derzeit anzuwendenden Richtlinie 95/46/EG ist es nämlich durchaus möglich, dass Bürger, die sich über die Verarbeitung personenbezogener Daten durch ein in mehreren Mitgliedstaaten tätiges Unternehmen beschweren möchten, sich an eine bestimmte Aufsichtsbehörde wenden müssen und, falls sie deren Entscheidungen anfechten möchten, den Rechtsstreit in eben diesem Mitgliedstaat führen müssen[9]. Unseres Wissens gibt es keinen Grund, dieses Merkmal des derzeitigen Systems mit der Charta der Grundrechte in Frage zu stellen.

Kritisiert wird der vorgeschlagene Grundsatz der zentralen Anlaufstelle auch, weil er angeblich übermäßig hohe Hindernisse für Bürger aufbaut, die gerichtlichen Rechtsbehelf in Anspruch nehmen wollen, und zwar aufgrund geografischer Entfernung, mangelnder Kenntnis der ausländischen Rechtsordnung, der Notwendigkeit der Klageerhebung und Führung des Verfahrens in einer Fremdsprache oder der Kosten eines solchen Verfahrens.

Die hierzu vorgeschlagene Alternative scheint die Einrichtung einer EU-Einrichtung mit eigener Rechtspersönlichkeit zu sein, die die Funktion der zentralen Anlaufstelle übernehmen würde. Vom Konzept her könnte die Errichtung einer solchen „Datenschutzagentur“ auf EU-Ebene durchaus verlockend sein. Hierfür wäre allerdings eine grundlegende Zentralisierung der bestehenden dezentralen Struktur der Aufsicht im Datenschutz erforderlich, die – zumindest – einen zeitnahen Entscheidungsprozess nicht erleichtern würde.

Wichtiger ist jedoch, dass sie für einen besseren Schutz der Grundrechte von Bürgern nicht erforderlich ist.

Es ist zu bedenken, dass in den meisten Fällen alle relevanten Akteure – betroffene Personen, für die Verarbeitung Verantwortlicher und Aufsichtsbehörde – auch weiterhin in einem Land ansässig sind. Folglich würde der Grundsatz der zentralen Anlaufstelle nur in relativ wenigen Situationen zum Tragen kommen. Mit anderen Worten: Auch wenn einige dieser Fälle möglicherweise große Auswirkungen haben können, würde in der Praxis die Zahl der Fälle, in denen Bürger von Entscheidungen einer Aufsicht führenden Behörde mit Sitz in einem anderen Mitgliedstaat als ihren Wohnsitzmitgliedstaat betroffen sind, deutlich niedriger ausfallen als die Zahl der Fälle, in denen die „eigene“ Aufsichtsbehörde Entscheidungen trifft.

Schließlich muss der Grundsatz der zentralen Anlaufstelle in seinem eigenen Kontext als ein wichtiges Element gesehen werden, das zu Wirksamkeit und Kohärenz des künftigen Datenschutzrahmens beiträgt. Ganz ohne Zweifel würden sich ein einheitlicheres Datenschutzsystem und niedrigere Prozesskosten (denn Gerichtsverfahren wären auf die Rechtsordnung der Aufsicht führenden Behörde beschränkt, also auf das Land der Hauptniederlassung) für die Unternehmen in der gesamten EU vorteilhaft auswirken. Allerdings werden **auch die Bürger** von einer kohärenteren Anwendung eines einheitlichen Datenschutzregelwerks **Nutzen haben**, wie es in der vorgeschlagenen Datenschutz-Grundverordnung vorgesehen ist.

Ist beispielsweise ein Bürger von einer Datenverarbeitung durch eine (Neben-)Niederlassung im eigenen Land (und möglicherweise durch andere Niederlassungen) betroffen, werden aber alle Entscheidungen von der Hauptniederlassung des für die Verarbeitung Verantwortlichen in einem anderen Mitgliedstaat getroffen, wäre die Möglichkeit, eine einzige Entscheidung

[9] Siehe z- B. den Fall Facebook und die irische Aufsichtsbehörde.

einer Aufsichtsbehörde oder ein Gerichtsurteil zu erwirken, die/das in allen diesen Mitgliedstaaten gültig und vollstreckbar wäre, im Vergleich zur heutigen Situation eine eindeutige Verbesserung.

Im Übrigen verringert die zentrale Anlaufstelle auch die Wahrscheinlichkeit von Parallelverfahren und daraus resultierender Kompetenzkonflikte, denn ein Verfahren im Mitgliedstaat der Aufsicht führenden Behörde würde normalerweise ausreichen, um Rechte in der gesamten EU durchzusetzen.

Dessen ungeachtet machen manche Fragen im Zusammenhang mit der künftigen Arbeitsweise der zentralen Anlaufstelle weitere Überlegungen erforderlich und müssen wichtige Einzelheiten noch genauer herausgearbeitet oder näher definiert werden. Wir sind gerne bereit, Ihnen hierbei bei Bedarf Hilfestellung zu leisten.

3. Risikogestützter Ansatz und Rechenschaftspflicht

Wiederholt haben wir die Aufnahme des Grundsatzes der Rechenschaftspflicht[10] in die vorgeschlagene Datenschutz-Grundverordnung begrüßt und unterstützt, dem zufolge der für die Verarbeitung Verantwortliche durch geeignete Strategien und Maßnahmen sicherzustellen hat, dass er sich an die Datenschutzvorschriften hält und er auch für die Überprüfung der Wirksamkeit der Maßnahmen zu sorgen hat[11]. Dieser Grundsatz soll dem für die Verarbeitung Verantwortlichen Ansporn sein, den Bürgern einen wirksamen Datenschutz zu gewährleisten und nicht nur ein System zu haben, in dem „Kästchen angeklickt" werden, um bürokratischen Anforderungen Genüge zu tun.

Rechenschaftspflicht bedeutet auch, dass Bemühungen um die Einhaltung der Vorschriften vorrangig in den Bereichen unternommen werden, in denen sie am nötigsten sind, wenn es beispielsweise um die besondere Schutzwürdigkeit der Daten oder die mit einer bestimmten Verarbeitung einhergehenden Risiken geht. In diesem Zusammenhang begrüßen wir die bisherigen Bemühungen mehrerer Ratsvorsitze um eine angemessene Beschreibung des Begriffs „Risiko", bei der zwangsläufig ein gewisser Beurteilungsspielraum besteht. Im Interesse der Rechtssicherheit sollte die vorgeschlagene Datenschutz-Grundverordnung hinreichend klare Kriterien vorgeben, anhand derer für die Verarbeitung Verantwortliche eine solche Risikobewertung vornehmen können; dabei sollten sowohl objektive Faktoren (wie z. B. die Zahl der von einer bestimmten Verarbeitung betroffenen Personen) als auch eher subjektive Faktoren (z. B. mögliche Beeinträchtigungen der Privatsphäre einer Person) herangezogen werden. Auf der Grundlage solcher allgemeinen Kriterien in der Datenschutz-Grundverordnung könnten weitere Orientierungshilfen entweder vom Europäischen Datenschutzausschuss oder gegebenenfalls in delegierten Rechtsakten gegeben werden. Ein solcher Ansatz böte größere Rechtssicherheit für den für die Verarbeitung Verantwortlichen, einen wirksameren Schutz für die EU-Bürger und ausreichend Flexibilität, um sich zu bewähren.

Wir stehen Ihnen auch weiterhin zur Beratung in den oben angesprochenen Fragen, aber auch zu anderen noch in der Diskussion befindlichen Fragen zur Verfügung, wenn Sie dies für sinnvoll halten, um den Reformprozess voranzubringen.

[10] Siehe Stellungnahme 3/2010 der Artikel 29-Datenschutzgruppe vom 13. Juli 2010 zum Grundsatz der Rechenschaftspflicht (WP 173).
[11] Artikel 22 des Vorschlags.

Eine Kopie dieses Schreibens wurde den Ständigen Vertretungen der Mitgliedstaaten, Herrn Juan Fernando LÓPEZ AGUILAR, Vorsitzender des LIBE-Ausschusses des Europäischen Parlaments, und Frau Viviane REDING, Vizepräsidentin der Europäischen Kommission, übermittelt.

Mit freundlichen Grüßen

(**unterzeichnet**)

Peter HUSTINX