EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 6/2015

Ein weiterer Schritt in Richtung eines umfassenden Datenschutzes in der EU

Empfehlungen des EDSB zur Datenschutzrichtlinie für Polizei und Justiz

28. Oktober 2015

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU. Der Datenschutzbeauftragte hat nach Artikel 41 Absatz 2 der Verordnung Nr. 45/2001 „im Hinblick auf die Verarbeitung personenbezogener Daten [...] sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden“ *und ist* „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten [zuständig].“

Der Datenschutzbeauftragte und der Stellvertretende Datenschutzbeauftragte wurden im Dezember 2014 mit dem konkreten Auftrag ernannt, konstruktiver und proaktiver vorzugehen, und haben im März 2015 eine Fünfjahresstrategie veröffentlicht, in der sie darlegten, wie sie diesen Auftrag umzusetzen und darüber Rechenschaft abzulegen gedenken[1].

Diese Stellungnahme stellt einen weiteren Meilenstein in der Strategie des EDSB dar, was die Tatsache unterstreicht, dass eine Reform der EU-Datenschutzvorschriften dringender denn je ist. Wie in der jüngsten Stellungnahme 3/2015 deutlich gemacht, ist der EDSB zusammen mit den nationalen Partner-Datenschutzbehörden ein aktiver Partner in den Diskussionen zur Datenschutzreform zwischen der Europäischen Kommission, dem Parlament und dem Rat. Allerdings wird er nicht am abschließenden Trilog zur Datenschutzrichtlinie für Polizei und Justiz teilnehmen. Wir werden weiterhin nach robusten, effektiven, praktikablen und tragfähigen Lösungen suchen. Diese Stellungnahme ist ein weiterer Ausdruck unseres Engagements. In den kommenden Wochen werden konkrete Empfehlungen zum entsprechenden Text des Richtlinienentwurfs folgen, der auch in die mobile EDSB-Datenschutz-App integriert werden wird.

Diese Stellungnahme zur Datenschutzrichtlinie für Polizei und Justiz steht im Einklang mit der umfassenden Stellungnahme des EDSB zu dem von der Kommission vorgeschlagenen Reformpaket vom März 2012. Die in dieser Stellungnahme dargelegten Standpunkte bleiben weiterhin gültig. Mehr als dreieinhalb Jahre später mussten wir allerdings unsere Empfehlung auf den neuesten Stand bringen, um uns unmittelbarer mit den Positionen der Mitgesetzgeber auseinandersetzen und konkrete Empfehlungen abgeben zu können [2]*. Wie die Stellungnahme aus dem Jahr 2012 steht auch diese Stellungnahme im Einklang mit den Meinungen und Aussagen der Artikel 29-Datenschutzgruppe.*

Inhaltsverzeichnis

I. Diese Richtlinie ist ein wichtiger Schritt in Richtung eines modernen Datenschutzes in der EU

Mit der Annahme des allgemeinen Übereinkommens zur Datenschutzrichtlinie für Polizei und Justiz[3] hat der Rat einen Schritt in Richtung eines neuen Rahmens für den Datenschutz in der EU getan.

Einer der Hauptmängel der derzeitigen EU-Datenschutzgesetze in diesen Bereichen ist, dass es sich um ein Flickwerk handelt, das aus verschiedenen Vorschriften für die spezifischen Bereiche sowie einem Instrument besteht, das allgemein anwendbar sein sollte, dies jedoch nicht ist. Der Rahmenbeschluss des Rates über den Datenschutz aus dem Jahr 2008[4] findet tatsächlich nur dann Anwendung, wenn Daten zwischen den Mitgliedstaaten ausgetauscht werden, nicht jedoch für Daten auf nationaler Ebene. Die vorliegende Richtlinie könnte zur Folge haben, dass die europäischen Bürger endlich von einem aktualisierten Rechtsinstrument der Union profitieren können, das für alle Polizei- und Justizbereiche gültig sein wird.

Der vorliegende Vorschlag wird auch begrüßt, da er die Notwendigkeit eines umfassenden Datenschutzes bekräftigt. Wenn mit der allgemeinen Datenschutzverordnung die Rechtsvorschriften im privaten Sektor und ein Großteil des öffentlichen Sektors modernisiert werden sollen, wäre es nicht annehmbar, dass die Polizei- und Justizbereiche, in denen so viele sensible personenbezogene Daten verarbeitet werden, im Rahmen der derzeitigen Gesetzesänderungen nicht aktualisiert würden. Ein umfassendes Schutzsystem wird ebenfalls benötigt, da in unseren modernen Gesellschaften große Mengen an personenbezogenen Daten zwischen den verschiedenen Bereichen ausgetauscht werden.

Diese Notwendigkeit der Vollständigkeit ist auch ein Grund, weshalb der EDSB nachdrücklich das gleichzeitige Inkrafttreten der verschiedenen Instrumente der Datenschutzreform empfiehlt. In diesem Zusammenhang

1. sollte die zweijährige Umsetzungsfrist der Richtlinie, wie von der Kommission vorgeschlagen, beibehalten werden und nicht auf drei Jahre verlängert werden.
2. sollte die Kommission so bald wie möglich Ihren Vorschlag für ein neues Instrument für den Datenschutz auf Ebene der Organe und Einrichtungen der EU vorlegen und die Verordnung 45/2001 mit diesem ersetzen.

II. Die Vorschriften sollten ein hohes Schutzniveau gewährleisten

Mit unserer Forderung nach Vollständigkeit soll außerdem sichergestellt werden, dass die für alle Bereiche der Gesellschaft geltenden Vorschriften einheitlich sind und ein hohes Schutzniveau gewährleisten. Ein hohes Schutzniveau ist erforderlich, da das Recht auf Datenschutz im EU-Primärrecht verankert ist, insbesondere in Artikel 16 AEUV und Artikel 8 der Charta der Grundrechte der Europäischen Union. Der Datenschutz steht in engem Zusammenhang mit dem Recht auf Privatsphäre, einem grundlegenden Wert in unseren demokratischen Gesellschaften, der bereits 1950 in der Europäischen Menschenrechtskonvention rechtlich anerkannt wurde, und nun auch in Artikel 7 der Charta verankert ist.

Die Urteile des Gerichtshofes in der Rechtssache *Digital Rights Ireland*[5] und jüngst bei *Schrems*[6] sind ein weiterer Beleg für die Notwendigkeit eines hohen Schutzniveaus, insbesondere im Zusammenhang mit der Durchsetzung von Rechtsvorschriften und der nationalen Sicherheit. Im *Digital Rights Ireland*-Urteil warnt der Gerichtshof davor, dass das Instrument zur Vorratsspeicherung von Daten geeignet ist, „*bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist*“[7]. Im *Schrems*-Urteil gelangt der

Gerichtshof zu der Auffassung, dass eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des Grundrechts auf Achtung der Privatsphäre verletzt[8].

Hierbei handelt es sich lediglich um Beispiele für einen Ansatz in dem Vertrag und die Bestätigung des höchsten Gerichtshofs der EU, was die Notwendigkeit eines starken Schutzes natürlicher Personen als Teil der Werte der Europäischen Union unterstreicht. Derselbe Ansatz sollte in der Richtlinie berücksichtigt werden, in der nicht nur die gesetzlichen Vorschriften einzuhalten sind, die im internationalen Recht und im EU-Recht verankert sind, sondern in der auch dargelegt wird, dass Privatsphäre und Datenschutz grundlegende Werte für natürliche Personen und die Gesellschaft als solche darstellen.

In der Stellungnahme des EDSB zum Reformpaket vom März 2012 wurde insbesondere das Schutzniveau in der vorgeschlagenen Richtlinie kritisiert. Wir haben betont, dass das Schutzniveau höchst unzureichend war.

Die Hauptrechtfertigung für eine besondere Datenschutzregelung in den Polizei- und Justizbereichen bezieht sich auf den spezifischen Charakter dieser Bereiche[9]. Es sind also spezifische Vorschriften erforderlich und keine Vorschriften, die hauptsächlich Ausnahmen zu den Datenschutzgrundsätzen enthalten, die in der vorgeschlagenen allgemeinen Datenschutzverordnung festgelegt sind. Datenschutz in den Bereichen Polizei und Justiz sollte in vollem Einklang mit den allgemeinen Vorschriften stehen und nur dort Spezifizierungen enthalten, wo diese erforderlich sind.

Ferner soll mit dem allgemeinen Übereinkommen des Rates der Charakter der Richtlinie so geändert werden, dass ein Instrument entsteht, das ein Mindestmaß an Harmonisierung gewährleistet. Somit bleibt es den Mitgliedstaaten unbenommen, nach nationalem Recht strengere Datenschutzbestimmungen zu erlassen[10]. Wir sind nicht dagegen, dass den Mitgliedstaaten hinsichtlich strengerer Datenschutzbestimmungen auf nationaler Ebene ein Ermessensspielraum eingeräumt wird, dennoch betonen wir die Verantwortung des EU-Gesetzgebers, nach Artikel 16 AEUV hohe Datenschutzstandards zu gewährleisten und dies nicht den einzelnen Mitgliedstaaten zu überlassen. Eine Differenzierung der Standards zwischen den Mitgliedstaaten würde zudem den freien Informationsfluss zwischen den zuständigen Behörden behindern und somit die Wirksamkeit der polizeilichen und justiziellen Zusammenarbeit beeinträchtigen. Wenn sich die Standards der Mitgliedstaaten zu sehr unterscheiden, würde dies auch den Informationsaustausch mit Europol erschweren. Im Vergleich zur Richtlinie hat Europol seine eigene, relativ strenge Datenschutzregelung: Die Mitgliedstaaten können auf bilateraler Ebene auf der Grundlage des kleinsten gemeinsamen Nenners zusammenarbeiten.

Im Wesentlichen sollte der EU-Gesetzgeber sicherstellen, dass:

1. keine der Bestimmungen der Richtlinie das Schutzniveau verringert, das derzeit durch EU-Recht – insbesondere im Rahmenbeschluss des Rates aus dem Jahr 2008 – und durch die Instrumente des Europarats gewährt wird[11].
2. die wesentlichen Bestandteile des Datenschutzes, die in Artikel 8 der Charta der Grundrechte der Europäischen Union verankert sind, geachtet werden und dass Ausnahmen die im *Digital Rights Ireland*-Urteil[12] festgelegte, strenge Prüfung der Verhältnismäßigkeit bestehen müssen. In dieser Stellungnahme gehen wir insbesondere auf den Grundsatz der Zweckbindung, das Recht der Personen auf Zugang zu den sie betreffenden Daten sowie die Kontrolle durch unabhängige Datenschutzbehörden ein[13].

3. Die wesentlichen Bestandteile des Datenschutzes sind in der Richtlinie verankert und werden nicht dem Ermessen der Mitgliedstaaten überlassen[14].

III. Der Anwendungsbereich der Richtlinie sollte auf Bereiche beschränkt werden, in denen spezifische Vorschriften tatsächlich erforderlich sind

Wir stellen fest, dass in dem allgemeinen Übereinkommen über die Richtlinie des Rates der Anwendungsbereich auf den Schutz vor und zur Abwehr von Bedrohungen der öffentlichen Sicherheit ausgeweitet wird[15], ein Bereich außerhalb des Strafrechts, der nach geltendem Recht nicht vom derzeitigen Rahmenbeschluss des Rates über den Datenschutz abgedeckt ist. In Erwägungsgrund (11a) werden Beispiele genannt, die abgedeckt wären: polizeiliche Tätigkeiten bei Demonstrationen, sportlichen Großveranstaltungen und Ausschreitungen oder, allgemein, polizeiliche Tätigkeiten zur Aufrechterhaltung von Recht und Ordnung.

Die Definition von „*Schutz vor und die Abwehr von Bedrohungen der öffentlichen Sicherheit*“ bleibt jedoch unklar. Dieser Ausdruck kann unterschiedlich interpretiert werden und sorgt für keine klare Abgrenzung der Aufgaben der Polizei innerhalb des Anwendungsbereichs der Richtlinie[16]. Daher empfehlen wir, wie im ursprünglichen Vorschlag der Kommission, den Anwendungsbereich der Richtlinie auf Strafverfolgungstätigkeiten der Polizei- und Justizbehörden zu beschränken.

Nach Ansicht des EDSB sollte der Begriff „zuständige Behörde“, wie er in Artikel 3 Absatz 13 definiert ist, ebenfalls möglichst beschränkt bleiben: Die Durchführung von Strafverfolgungsaufgaben durch nichtöffentliche Einrichtungen und Organisationen sollte der Verordnung unterliegen und nicht der Richtlinie. Für diese privaten Einrichtungen und Organisationen ist keine spezielle Regelung erforderlich. Bei Fluggesellschaften oder Telekommunikationsunternehmen, die gesetzlich verpflichtet sind, ihre Daten herauszugeben, sollte die Richtlinie beispielsweise keine Anwendung finden, da sich der ursprüngliche Hauptzweck dieser Datenerhebung gänzlich von der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten unterscheidet. In Erwägungsgrund (11) des allgemeinen Übereinkommens des Rates wird zudem die Vorratsspeicherung von Daten durch Finanzinstitute genannt und in diesem speziellen Fall die Verpflichtung dieser privaten Einrichtungen, nach Artikel 21 der Richtlinie vertraglich gebunden zu sein.

Außerdem[17] wird in Artikel 2 Absatz 3 des Vorschlags die Verarbeitung personenbezogener Daten vom Anwendungsbereich ausgenommen, die für die Ausübung einer Tätigkeit erfolgt, die nicht in den Anwendungsbereich des Unionsrechts fällt. Der Verweis auf die nationale Sicherheit wurde in Artikel 2 Absatz 3 gestrichen, jedoch in Erwägungsgrund (11b) wieder eingefügt. Wie der EDSB bereits erklärt hat, ist nicht immer klar, was mit diesem Begriff abgedeckt wird, da dies von der nationalen Politik der Mitgliedstaaten abhängt. Wir nehmen die Ausnahme zur Kenntnis, sind jedoch der Auffassung, dass diese nicht herangezogen werden sollte, um die Verarbeitung personenbezogener Daten außerhalb des Anwendungsbereichs der Verordnung und der Richtlinie, wie beispielsweise im Rahmen der Terrorismusbekämpfung, zu legitimieren. Folglich,

1. sollte die Verordnung weiterhin für alle Tätigkeiten gelten, die nicht unmittelbar mit der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder mit der Vollstreckung strafrechtlicher Sanktionen in Verbindung stehen, sowie für Fälle, bei denen sich spezifische Vorschriften als notwendig erwiesen haben.

2. sollte die Durchführung von Strafverfolgungsaufgaben durch öffentliche Einrichtungen und Organisationen der Verordnung unterliegen.

IV. Zweckbindung und besondere Datenkategorien

Wir stellen fest, dass im allgemeinen Übereinkommen des Rates zur Richtlinie in Artikel 4 ein zweiter Paragraf hinzugefügt wurde, nach dem die Verarbeitung durch denselben oder einen anderen für die Verarbeitung Verantwortlichen zu anderen Zwecken als die, für die Daten erhoben wurden, zulässig ist, soweit der für die Verarbeitung Verantwortliche zur Verarbeitung solcher Daten für solche Zwecke nach den geltendem Rechtsvorschriften befugt ist, und die Verarbeitung für diesen anderen Zweck notwendig und verhältnismäßig ist. Wir betonen die Bedeutung der Achtung des Grundsatzes der Zweckbindung, der einen Eckpfeiler des Datenschutzrechts darstellt[18]. Es muss sichergestellt werden, dass die Daten, die die zuständigen Behörden im Rahmen der Richtlinie verarbeiten, nicht für gänzlich andere Zwecke weiterverwendet werden, was daher leicht als unvereinbar anzusehen ist (zum Beispiel die Weiterverwendung von Daten, die von der Polizei für Einwanderungszwecke erhoben wurden). Wir empfehlen, dass der Wortlaut durch zusätzliche Erwägungen ergänzt wird, um den Begriff Zweckbindung im Polizei- und Justizbereich einzugrenzen und den Begriff unvereinbare Weiterverarbeitung zu präzisieren. Ähnliche Überlegungen werden derzeit im Rahmen der Europol-Verordnung[19] entwickelt und wurden in der jüngsten Stellungnahme des EDSB zur allgemeinen Datenschutzverordnung (Artikel 6 Absatz 2) erwähnt.

Wir verweisen auch auf den Wortlaut der Einschränkung für die Verarbeitung besonderer Kategorien personenbezogener Daten in Artikel 8, der so formuliert werden sollte, dass die Verarbeitung dieser Datenkategorien untersagt ist, es sei denn, es gilt eine spezielle und ausdrückliche Ausnahmeregelung (wie im Wortlaut des Parlaments vorgeschlagen). Der Wortlaut sollte nicht so gewählt werden, dass das derzeitige Schutzniveau auf der Grundlage des Grundsatzes 2.4 der Empfehlung Nr. R (87) 15 des Europarats unterschritten wird. Im Wesentlichen

1. sollte genauer festgelegt werden, was Zweckbindung in den Polizei- und Justizbereichen bedeutet und was sich hinter dem Ausdruck unvereinbare Weiterverarbeitung verbirgt.
2. sollte die Verarbeitung besonderer Kategorien personenbezogener Daten in den Polizei- und Justizbereichen weiterhin untersagt bleiben, es sei denn, es gilt eine spezielle Ausnahmeregelung von Artikel 8 der Richtlinie.

V. Rechte der betroffenen Personen

Wir erinnern daran, dass die Rechte natürlicher Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten ein wesentlicher Bestandteil des in Artikel 8 der Charta verankerten Rechts auf Schutz der personenbezogenen Daten ist. Zu diesen Rechten zählt, dass die Personen über die Verarbeitung ihrer personenbezogenen Daten und über ihre Rechte informiert werden, um eine Verarbeitung nach Treu und Glauben zu gewährleisten und dass sie die Möglichkeit haben, Zugang zu Ihren Daten zu erhalten und um Berichtigung, Löschung oder Einschränkung der Bearbeitung zu bitten. Wir stellen fest, dass die in der allgemeinen Ausrichtung des Rates vereinbarten Bestimmungen die Rechte der Personen nicht in vollem Umfang garantieren, insbesondere in Fällen, bei denen eine Einschränkung der Rechte der Personen nicht, oder nicht mehr, gilt.

Daher fordern wir die Mitgesetzgeber auf, dafür zu sorgen, dass der Wortlaut in den Artikeln 10 bis 16 die Mindestanforderungen dieser Rechte einhält und dass das derzeitige Datenschutzniveau, das in der Charta, den EU-Verträgen und den internationalen Verträgen (insbesondere Übereinkommen Nr. 108) gewährleistet ist, nicht unterschritten wird.

Im Wortlaut sollte klargemacht werden, dass die Einschränkungen der Rechte der natürlichen Personen, bei denen es sich um Ausnahmen von einem Grundrecht handelt, wie von der Rechtssprechung des Gerichtshofs gefordert, restriktiv auszulegen sind. Diese Einschränkungen können zur Folge haben, dass die Übermittlung von Informationen an die Person im Einzelfall und in dem Ausmaß und so lange dies erforderlich ist, abgelehnt werden kann. Wenn die Einschränkung aufgehoben wird, sollte die Person jedoch ihre Rechte in vollem Umfang ausüben können. Ferner sollte die betroffene Person stets schriftlich über etwaige Ablehnungen oder Einschränkungen informiert werden. Die Übermittlung der Begründung darf nur eingeschränkt werden, wenn dies für einen der berechtigten Ablehnungsgründe erforderlich ist. Im Wesentlichen

1. sollte der ursprüngliche Wortlaut von Artikel 10 des Kommissionsvorschlags über die Übermittlung und Modalitäten zur Ausübung der Rechte der betroffenen Person wieder hergestellt werden, da in der allgemeinen Ausrichtung des Rates wesentliche Bestandteile gestrichen wurden.
2. sollte die Unterrichtung der Personen zudem Informationen über Folgendes enthalten (i) den für die Daten geltenden Speicherzeitraum, (ii) das Recht auf Zugang, Berichtigung, Löschung oder Einschränkung und (iii) die Empfängerkategorie, einschließlich Dritter oder internationaler Organisationen wie in Artikel 11 des Kommissionsvorschlags vorgesehen.
3. sollte das Zugangsrecht fest in Artikel 12 verankert sein und nicht in Abhängigkeit der in den einzelstaatlichen Rechtsvorschriften vorgesehenen Abweichungen ausgeübt werden (wie dies in Artikel 12 Absatz 1 der allgemeinen Ausrichtung des Rates vorgesehen ist). Das Gegenteil ist der Fall: Das Recht auf Zugang sollte grundsätzlich gewährt werden und davon darf nur unter bestimmten Umständen abgewichen werden, die ausdrücklich im Gesetz vorgesehen sind, und für die Zeit, in der diese Einschränkungen gelten.

VI. Gewährleistung der Kontrolle durch unabhängige Datenschutzbehörden

Wir sind der Auffassung, dass eine Differenzierung zwischen den Befugnissen, die den Datenschutzbehörden (Data Protection Authorities, DPA) gemäß der Verordnung und Richtlinie übertragen wurden, nicht erforderlich ist. Überwachung ist ein wesentlicher Bestandteil des Grundrechts auf Datenschutz[20] und das Ausmaß und die Intensität der Überwachung sollten nicht von dem Bereich abhängig sein, in dem die personenbezogenen Daten verarbeitet werden.

Wir stellen fest, dass die durch die Richtlinie verliehenen Befugnisse der Aufsichtsbehörden nicht mit den in Artikel 53 aufgelisteten Befugnissen der vorgeschlagenen Verordnung abgestimmt sind[21]. Die Befugnis zur Verhängung von Sanktionen wird beispielsweise nur vom Europäischen Parlament aufgenommen, wohingegen die Verordnung eine solche Möglichkeit vorsieht. Ein weiteres Beispiel ist die fehlende Spezifikation der Untersuchungsbefugnisse der Aufsichtsbehörden, die im Vergleich zu den in der vorgeschlagenen Verordnung vorgesehenen Untersuchungsbefugnissen nicht verringert werden sollten.

Die Möglichkeit, die Gerichte, in Ausübung ihrer Rechtsprechungsbefugnisse, von der Überwachung auszuschließen, wirft ernste Fragen hinsichtlich der Interpretation und des

Anwendungsbereichs auf[22]. Daher empfehlen wir, unter Bezugnahme auf Erwägungsgrund 55 des Vorschlags der Kommission, den vom Rat gestrichenen Begriff „**echte**“ justizielle Tätigkeiten, beizubehalten. Wie in Erwägungsgrund betont, ist *Sinn und Zweck* der Ausnahme in Artikel 44 Absatz 2 offenbar, die „*Unabhängigkeit der Richter bei der Ausübung ihrer justiziellen Aufgaben zu gewährleisten*“[23]. Insbesondere unter Berücksichtigung der erheblichen Unterschiede zwischen den Rechtssystemen der Mitgliedstaaten, stellen wir in diesem Zusammenhang außerdem fest, dass nicht immer klar ist, ob und wann Staatsanwälte „unabhängige Justizbehörden“ sind und wann und in welchem Umfang ihre Tätigkeiten „justizielle Tätigkeiten“ darstellen. Daher sind entsprechende Klarstellungen erforderlich.

Gemäß der vorgeschlagenen Verordnung, wird der Europäische Datenschutzausschuss (European Data Protection Board, EDPB) aus einer Aufsichtsbehörde eines jeden Mitgliedstaates sowie dem EDSB bestehen. Gemäß Artikel 39 Absatz 2 der vorgeschlagenen Richtlinie handelt es sich bei der Aufsichtsbehörde jedoch nicht zwangsweise um die Aufsichtsbehörde, die in der vorgeschlagenen Verordnung bestimmt wurde. Daher muss nicht unbedingt ein Mitglied des EDSB für die Überwachung innerhalb des Anwendungsbereichs der Richtlinie zuständig sein. Wir empfehlen, diesen Punkt klarzustellen, indem beispielsweise in Artikel 39 Absatz 3 festgelegt wird, dass für den Fall, dass verschiedene Behörden gemäß der Verordnung und der Richtlinie benannt werden, diese Ihre Tätigkeiten aufeinander abstimmen sollten, um die Meinung beider Behörden beim EDSB zu vertreten. Im Wesentlichen

1. ist eine Differenzierung zwischen den Befugnissen, die den DPA gemäß der Verordnung und Richtlinie übertragen wurden, nicht erforderlich.
2. sollte die Ausnahme von Aufsichtsbefugnissen der DPA im Justizbereich auf „echte“ justizielle Tätigkeiten eingeschränkt werden, auch durch Klarstellung der Position der Staatsanwaltschaften.

VII. Internationale Übermittlungen und Übermittlungen an nichtöffentliche Stellen

Das *Schrems*-Urteil[24] bestätigt die strengen Bedingungen für die Übermittlung von personenbezogenen Daten an Drittstaaten. Wir empfehlen die erneute Überprüfung von Kapitel V der Richtlinie unter gebührender Beachtung des Schrems-Urteils. Dies bedeutet beispielsweise, dass eine Angemessenheitsentscheidung nur auf Grundlage einer umfassenden Beurteilung der Strafverfolgungsbehörden getroffen werden kann. Eine Angemessenheitsentscheidung sollte der Aufsichtsbehörde nicht die Befugnis entziehen, eine bestimmte Übermittlung zu überprüfen und Durchsetzungsmaßnahmen zu ergreifen, falls die Übermittlung nicht den erforderlichen Standard erfüllt.

Außerdem empfehlen wir sicherzustellen, dass die Übermittlung von personenbezogenen Daten ohne eine Angemessenheitsentscheidung auf Situationen beschränkt wird, in denen ein rechtsverbindliches Instrument vorliegt, oder die Notwendigkeit besteht, das grundlegende Interesse der betroffenen Person zu schützen, oder für den Fall einer unmittelbaren und schwerwiegenden Gefährdung der öffentlichen Sicherheit[25]. Wir empfehlen, Artikel 34 Absatz 6 und Artikel 36 entsprechend anzupassen.

Schließlich sind wir der Auffassung, dass die Übermittlung an eine nichtöffentliche Stelle nur gemäß den derzeit in der Empfehlung Nr. R (87) 15 des Europarats festgelegten Bestimmungen erfolgen darf. Die Übermittlung sollte nur stattfinden, wenn sie zweifelsfrei im Interesse der betroffenen Person ist und die betroffene Person entweder zugestimmt hat oder die Umstände eindeutig eine solche Einwilligung vermuten lassen oder wenn die Übermittlung zur Abwehr

einer ernsthaften und unmittelbaren Gefahr erforderlich ist. Wir empfehlen, Artikel 36 Buchstabe aa entsprechend des Vorschlags des Rates anzupassen. Im Wesentlichen

1. empfehlen wir die erneute Überprüfung von Kapitel V der Richtlinie, auch unter gebührender Beachtung des Schrems-Urteils.
2. dürfen Übermittlungen an eine nichtöffentliche Stelle nur gemäß den derzeit in der Empfehlung Nr. R (87) 15 des Europarats festgelegten Bestimmungen erfolgen.

VIII. Schlussbestimmungen

In der Stellungnahme wurde bereits erwähnt, dass, um sicherzustellen, dass ein umfassendes Datenschutzsystem in der Union erforderlich ist, die Richtlinie zur selben Zeit wie die allgemeine Datenschutzverordnung in Kraft treten sollte. Dasselbe Argument gilt für die Notwendigkeit sicherzustellen, dass bestehende Instrumente mit Vorschriften zum Datenschutz die Anforderungen der Richtlinie erfüllen.

Wir stellen fest, dass die Richtlinie gemäß dem Kommissionsvorschlag bestehende interne EU-Instrumente unberührt lässt, die Kommission jedoch dazu verpflichtet ist festzustellen, ob diese Instrumente innerhalb von zwei Jahren nach Annahme der Richtlinie mit dieser abgestimmt werden müssen (Artikel 61 Absatz 2). Der Rat schlägt vor, diese Frist auf fünf Jahre nach der Annahme zu verlängern. Dies würde den Zeitraum der Rechtsunsicherheit unangemessen verlängern.

Ferner streicht der Rat die Verpflichtung, falls erforderlich, bestehende Vereinbarungen zur Übermittlung von personenbezogenen Daten, die von den Mitgliedstaaten getroffen wurden, zu ändern. Im allgemeinen Übereinkommen des Rates wird hingegen festgelegt, dass alle Vereinbarungen, die vor dem Inkrafttreten der Richtlinie getroffen wurden, unberührt bleiben. Dies könnte nicht nur bedeuten, dass Vorschriften in diesen Vereinbarungen, die nicht der Richtlinie entsprechen, auf unbegrenzte Zeit in Kraft bleiben, sondern auch, dass die Mitgliedstaaten während der Umsetzungsfrist der Richtlinie befugt sind, Vereinbarungen mit Drittländern zu treffen, ohne den wesentlichen Inhalt der Richtlinie zu berücksichtigen[26]. Im Wesentlichen

1. sollte sichergestellt werden, dass so bald wie möglich überprüft wird, ob die bestehenden internen EU-Instrumente mit der Richtlinie abgestimmt werden müssen. Dies sollte in jedem Fall innerhalb von zwei 2 Jahren nach ihrem Inkrafttreten geschehen.
2. sollten, falls erforderlich, bestehende Vereinbarungen zur Übermittlung von personenbezogenen Daten, die von den Mitgliedstaaten getroffen wurden, innerhalb einer bestimmten Frist geändert werden. sollte es den Mitgliedstaaten während der Umsetzungsfrist der Richtlinie verwehrt sein, Vereinbarungen mit Drittländern zu treffen.

Brüssel, den 28. Oktober 2015

(unterzeichnet)

Giovanni BUTTARELLI
Europäischer Datenschutzbeauftragter

Anmerkungen

[1] Stellenausschreibung für den Europäischen Datenschutzbeauftragten KOM/2014/10354 (2014/C 163 A/02), ABl. C 163 A/6 vom 28.5.2014. In der Strategie des EDSB für 2015-2019 wurde die „*Suche nach tragfähigen Lösungen, bei denen Verwaltungsaufwand vermieden wird, die mit Blick auf technologische Innovationen und grenzüberschreitende Datenströme flexibel sind und es natürlichen Personen ermöglichen, ihre Rechte online und offline wirksamer durchzusetzen*“ versprochen. Mit gutem Beispiel vorangehen: Strategie des EDSB für 2015-2019, März 2015.

[2] Stellungnahme des EDSB zum Datenschutzreformpaket, 7.3.2015.

[3] Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr KOM(2012)10 endgültig; Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, P7_TA(2014)0219.

[4] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350/60.

[5] Verbundene Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland (C-293/12) und Seitlinger (C-594/12), ECLI:EU:C:2014:238.

[6] Rechtssache C-362/14, Schrems, ECLI:EU:C:2015:650.

[7] Verbundene Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland (C-293/12) und Seitlinger (C-594/12), ECLI:EU:C:2014:238, Rn. 37.

[8] Rechtssache C-362/14, Schrems, ECLI:EU:C:2015:650, Rn. 94.

[9] Siehe z. B. Erklärung (21) zum Schutz personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit im Anhang des Vertrages von Lissabon: *„Die Konferenz erkennt an, dass es sich aufgrund des spezifischen Charakters der Bereiche justizielle Zusammenarbeit in Strafsachen und polizeiliche Zusammenarbeit als erforderlich erweisen könnte, in diesen Bereichen spezifische, auf Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gestützte Vorschriften über den Schutz personenbezogener Daten und den freien Datenverkehr zu erlassen“*.

[10] Artikel 1 Buchstabe a des allgemeinen Übereinkommens.

[11] Dies wird auch immer wieder vom Berichterstatter für die allgemeine Datenschutzverordnung betont. Siehe z. B. Jan Philipp Albrecht, No EU Data Protection Standard Below the Level of 1995, EDPL 2015, 1, Rn. 3-4.

[12] Verbundene Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland (C-293/12) und Seitlinger (C-594/12), ECLI:EU:C:2014:238.

[13] Kontrolle ist ein wesentlicher Bestandteil des Schutzes natürlicher Personen: Erwägungsgrund (62) der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281/31 sowie die jüngste Rechtsprechung des Gerichtshofes, Rechtssache C-362/14, Schrems, EU:C:2015:650, Rn. 42.

[14] Dies würde nicht im Einklang mit der Rechtsprechung des Gerichtshofes stehen, insbesondere nicht mit den verbundenen Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland (C-293/12) und Seitlinger (C-594/12), ECLI:EU:C:2014:238, Rn. 54-62.

[15] Artikel 1 Absatz 1 des allgemeinen Übereinkommens.

[16] Würden beispielsweise die Weiterverfolgung eines Selbstmordversuchs oder ein verwaltungsrechtlich verfügter Arrest in den Anwendungsbereich fallen?

[17] Wie in der Stellungnahme des EDSB zum Datenschutzreformpaket, 7.3.2015 hervorgehoben.

[18] Siehe Stellungnahme 03/2013 der Artikel 29-Datenschutzgruppe zur Zweckbindung, angenommen am 2. April 2013.

[19] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für die Zusammenarbeit und die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (Europol) und zur Aufhebung der Beschlüsse 2009/371/JI und 2005/681/JI.
[20] Wie jüngst in der Rechtssache C-362/14, Schrems, ECLI:EU:C:2015:650 bestätigt.
[21] Siehe auch Stellungnahme des EDSB zum Datenschutzreformpaket, 7.3.2015, Rn. III.8.
[22] Siehe auch Stellungnahme des EDSB zum Datenschutzreformpaket, 7.3.2015, Rn. III.8.
[23] Laut EDSB sollte sich das Kriterium hinsichtlich der Datenverarbeitung für den Ausschluss oder die Einbindung der Überwachung durch die DPA eher darauf stützen, ob die Verarbeitung personenbezogener Daten im Zusammenhang mit der justiziellen Tätigkeit stattfindet („Prozess", gerichtliches Verfahren, justizielle Tätigkeiten in Gerichtsverfahren) oder im Zusammenhang mit anderen Tätigkeiten steht, an denen Richter möglicherweise nach nationalem Recht beteiligt sind, als auf eine generelle Unterscheidung zwischen Kategorien der für die Datenverarbeitung Verantwortlichen, nämlich dem Gericht auf der einen Seite und dem Staatsanwalt als Beispiel für eine „andere Justizbehörde" auf der anderen Seite.
[24]Rechtssache C-362/14, Schrems, ECLI:EU:C:2015:650.
[25] Siehe auch Stellungnahme des EDSB zum Datenschutzreformpaket, 7.3.2015, Rn. III.7.
[26] kann die Befugnis unter bestimmten Voraussetzungen nach dem Grundsatz der loyalen Zusammenarbeit (Artikel 4 Absatz 3 EUV) eingeschränkt werden.