29. Juli 2015

Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung

I. Vorbemerkung

Nachdem der Rat der Justiz- und Innenminister am 15. Juni 2015 seinen Standpunkt zur Datenschutz-Grundverordnung abgeschlossen hat, beraten Kommission, Parlament und Rat seit Ende Juni im sogenannten Trilog über ihre verschiedenen Positionen zur Datenschutz-Grundverordnung mit dem Ziel einer Gesamteinigung und Verabschiedung des Rechtsaktes zum Jahresende 2015.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich seit der Präsentation der Vorschläge durch die Kommission im Januar 2012 mehrfach öffentlich zur Datenschutzreform positioniert. Sie hat sowohl zum gesamten Paket am 11. Juni 2012 eine Stellungnahme abgegeben als auch in einer Reihe von Entschließungen und Stellungnahmen zu einzelnen Fragen der Datenschutzreform Position bezogen[1]. Die Konferenz hat von Anfang an das Ziel der Kommission unterstützt, einen „modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union bereitzustellen“[2]. Dies gilt umso mehr, als die Kommission ausdrücklich das Grundrecht des Einzelnen auf Datenschutz in den Mittelpunkt gerückt hat, dem die Reform zugutekommen soll.

Deshalb ist es für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder von außerordentlicher Bedeutung, dass die Datenschutz-Grundverordnung im Vergleich zum geltenden Rechtsstand – der im Wesentlichen durch die Richtlinie 95/46/EG geprägt ist – einen verbesserten, mindestens aber gleichwertigen Grundrechtsschutz gewährleistet. Keinesfalls darf die Reform des Europäischen Datenschutzrechts dazu führen, hinter dem geltenden Datenschutzniveau zurückzubleiben. Die Konferenz betont, dass die sich aus Artikel 8 der Grundrechtecharta und Art. 16 Abs. 1 AEUV ergebenden Grundprinzipien des Datenschutzes daher nicht zur Disposition stehen dürfen. Nach wie vor fehlen spezifische

---

[1] Entschließungen „Ein hohes Datenschutzniveau für ganz Europa“ vom 21./22.3.2012 sowie Stellungnahme vom 11.6.2012; „Europäische Datenschutzreform konstruktiv und zügig voranbringen!“ vom 8./9.11.2012; „Europa muss den Datenschutz stärken“ nebst Erläuterungen vom 13./14.3.2013; „Zur Struktur der Europäischen Datenschutzaufsicht“ vom 27./28.3.2014 sowie „Datenschutz-Grundverordnung darf keine Mogelpackung werden!“ vom 18./19.3.2015, jeweils abrufbar unter http://www.bfdi.bund.de/DE/Infothek/Entschliessungen/DSBundLaender/Functions/DSK_table.html

[2] Mitteilung der Kommission Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endg., Ziff. 6

Anforderungen an riskante Datenverarbeitungen, wie z.B. beim Profiling oder bei der Videoüberwachung. Auch sollen Daten für Werbezwecke weiterhin ohne Einwilligung der Betroffenen verarbeitet werden können. Gerade in Zeiten von Big Data und globaler Datenverarbeitung sind die Autonomie des Einzelnen, Transparenz und Rechtmäßigkeit der Datenverarbeitung, die Zweckbindung oder die Verantwortlichkeit des Datenverarbeiters ebenso wichtige Elemente der Grundrechtsgewährleistung wie eine starke Datenschutzaufsicht und wirksame Sanktionen.

Bei den genannten und den im Folgenden angesprochenen Themen handelt es sich um die wichtigsten Punkte, denen sich nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die am Trilog teilnehmenden Parteien insbesondere widmen sollten.

Zur besseren Handhabbarkeit orientiert sich diese Stellungnahme an der Struktur der vorliegenden Entwürfe der Datenschutz-Grundverordnung.

II. Die Vorschläge im Einzelnen

1. Der Anwendungsbereich der Datenschutz-Grundverordnung

a. Keine Ausweitung der Haushaltsausnahme!

Der Rat hat die so genannte Haushaltsausnahme in Art. 2(2)(d) Datenschutz-Grundverordnung (DSGVO) in der Weise erweitert, dass er die im Kommissionsvorschlag enthaltenen Worte „ausschließlich“ und „ohne jede Gewinnerzielungsabsicht“ gestrichen hat.

Der Vorschlag des Rates ist in einer Weise formuliert, dass ein maßgeblicher Teil der Verarbeitung personenbezogener Daten durch natürliche Personen auch dann aus dem Anwendungsbereich des Datenschutzrechts herausfiele, wenn in erheblicher Weise in das Datenschutzgrundrecht Dritter eingegriffen würde. Nach der Formulierung des Rates würde es bereits genügen, wenn die Verarbeitung zu persönlichen oder familiären Zwecken bei einer Gesamtbetrachtung lediglich einen völlig untergeordneten Zweck darstellte, um unter die Haushaltsausnahme zu fallen und damit nicht mehr dem Datenschutzrecht zu unterliegen. Ein Nutzer eines sozialen Netzwerks oder der Betreiber einer privaten Homepage würde selbst dann nicht unter das Datenschutzrecht fallen, wenn er in großem Umfang personenbezogene Daten unbeschränkt im Internet veröffentlicht, solange er die Datenverarbeitung (auch) als eine solche zu persönlichen oder familiären Zwecken deklariert. Eine derartige Erweiterung wäre nicht akzeptabel. Ebenso wenig kann die Gewinnerzielungsabsicht ein Kriterium für die Anwendung des Datenschutzrechts sein, da die Eingriffstiefe einer Datenverarbeitung hiervon nicht abhängt. Eine zu weitgehende Ausdehnung der Haushaltsausnahme stünde im Widerspruch zum primärrechtlich

garantierten Grundrecht auf Datenschutz und kann deshalb im Sekundärrecht nicht umgesetzt werden.

Die Konferenz spricht sich gegen eine Erweiterung der Haushaltsausnahme in Art. 2(2)(d) DSGVO und die damit verbundene Einschränkung des Anwendungsbereichs des Datenschutzrechts aus. Die Haushaltsausnahme sollte sich daher weiterhin an dem Wortlaut von Art. 2(2) der Richtlinie 95/46/EG orientieren und nur solche Verarbeitungsvorgänge aus dem Anwendungsbereich herausnehmen, die sich ausschließlich auf persönliche und familiäre Tätigkeiten beziehen.

b. Keine weitere Beschränkung des Anwendungsbereichs der DSGVO zugunsten der JI-Richtlinie!

Die DSGVO wird keine Anwendung finden, soweit die Richtlinie für den Bereich Polizei und Justiz (JI-RL) Anwendung finden wird. Somit bestimmt der Anwendungsbereich der JI-RL zugleich den Anwendungsbereich der DSGVO. Vor diesem Hintergrund hat der Rat in den letzten Monaten verschiedene Entwürfe diskutiert, die teilweise zu einer deutlichen Ausdehnung des Anwendungsbereichs der JI-RL führen könnten.

Die Konferenz sieht keine überzeugenden Gründe dafür, von der ursprünglich vorgesehenen Trennung der Anwendungsbereiche von DSGVO und der JI-RL wesentlich abzuweichen. Nach dem ursprünglichen Entwurf der KOM enthält die JI-RL Regelungen 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". Der Rat kritisiert, dass damit die präventive Gefahrenabwehr nicht erfasst ist, soweit sie der Prävention einer Straftat dient. Dies führe wiederum dazu, dass die Datenverarbeitung der Polizeien unterschiedlichen Rechtsakten unterliege. Um die gesamte Aufgabenerfüllung der Polizei unter einem Rechtsakt – der JI-RL – zusammenzufassen, soll der Anwendungsbereich der RL entsprechend erweitert werden. Dabei steht sogar im Raum, auch die Datenverarbeitung der Ordnungsverwaltung unter die RL zu fassen.

Eine solche Ausweitung lehnt die Konferenz ab. Sofern überhaupt ein Kompromiss gefunden werden muss, der den Anwendungsbereich der JI-RL für die polizeiliche Datenverarbeitung erweitern soll, muss durch die Formulierung im Gesetzestext und in den Erwägungsgründen zumindest sichergestellt sein, dass davon nicht auch noch die Datenverarbeitung der Ordnungsverwaltung erfasst wird. Die Datenverarbeitung von anderen Behörden muss weiterhin von der DSGVO geregelt werden, wie es auch der gegenwärtige Rechtsrahmen vorsieht.

Die Konferenz spricht sich gegen die in der Ratsfassung hinzugefügte Beschränkung des Anwendungsbereichs der DSGVO zugunsten der JI-Richtlinie in Art. 2(2)(e) DSGVO aus. Die

Datenverarbeitung der Ordnungsverwaltung und zur Gefahrenabwehr sollte von der DSGVO geregelt werden.

2. Für eine klare Definition des Personenbezugs!

Die DSGVO knüpft wie auch das geltende Recht weiterhin am Begriff des personenbezogenen Datums an. Dies ist die logische Konsequenz aus der grundrechtlichen und primärrechtlichen Gewährleistung in Art. 8 Abs. 1 EU-Grundrechtecharta und Art. 16 Abs. 1 AEUV, wonach jede Person das Recht auf Schutz der sie betreffenden Daten hat. Deshalb kommt der Definition des personenbezogenen Datums in Art. 4(1) DSGVO eine außerordentlich hohe Bedeutung zu, denn sie entscheidet letztlich über die Anwendbarkeit des Datenschutzrechts.

Dabei muss klargestellt sein, dass eine natürliche Person auch dann als identifizierbar anzusehen ist, wenn sie innerhalb einer Gruppe von Personen von anderen Personen unterschieden und damit auch unterschiedlich behandelt werden kann. Deshalb muss die Identifizierbarkeit einer Person auch deren Herausgreifen einschließen, wie es dem Vorschlag des Parlaments in EG 23 zugrundeliegt.

Die Vorschläge von Kommission und Rat zu EG 24 führen zudem zu einer unnötig restriktiven Auslegung des Begriffs des personenbezogenen Datums, indem sie Kennnummern, Standortdaten, Online-Kennungen oder IP-Adressen nicht notwendigerweise als personenbezogene Daten ansehen. Für diese Daten gelten die gleichen Kriterien für die Bestimmung des Personenbezugs wie für jede andere Information. Deren gesonderte Erwähnung verleitet zu dem unzulässigen Schluss, dass hier andere Kriterien gelten würden. Dies widerspräche auch der Rechtsprechung des EuGH.

Die Konferenz unterstützt insoweit den Vorschlag des Parlaments zu EG 23, wonach klargestellt ist, dass die Möglichkeit des Herausgreifens einer natürlichen Person aus einer Gruppe ein Mittel zu deren Identifizierbarkeit ist.

Die Konferenz fordert, bei EG 24 dem Vorschlag des Parlaments zu folgen, der klarstellt, dass Kennnummern, Standortdaten, Online-Kennungen, IP-Adressen oder sonstige Elemente grundsätzlich als personenbezogene Daten zu betrachten sind.

3. Datensparsamkeit muss Gestaltungsziel bleiben!

Für eine möglichst grundrechtsschonende Datenverarbeitung ist es unabdingbar, dass sich Staat und Wirtschaft auf das zur Erreichung ihrer rechtlichen oder legitimen Zwecke notwendige Maß beschränken. Die allgegenwärtige Datenverarbeitung und der Einsatz von

Big-Data-Technologien erzeugen eine unvorstellbare Menge an (auch personenbezogenen) Daten. Dies führt zu einer für viele als diffus bedrohlich empfundenen Situation, da auf diese Weise Unternehmen oder Behörden potentiell in der Lage sind, über jeden Einzelnen Informationen aus sämtlichen Lebensbereichen zu erfassen und beliebig auszuwerten. Gerade deshalb ist das Prinzip von Datenvermeidung und Datensparsamkeit, das seit vielen Jahren im deutschen Datenschutzrecht verankert ist, wichtiger denn je. Auf diese Weise werden Anreize für eine datenschutzfreundliche Gestaltung von Verarbeitungs- und Geschäftsprozessen geschaffen.

Dies haben die Kommission und das Parlament erfreulicherweise auch erkannt, indem sie das Prinzip der Datensparsamkeit ausdrücklich als eines der Grundprinzipien des Datenschutzes in Art. 5(1)(c) DSGVO verankert haben. Umso unverständlicher ist es, dass der Rat in seinem Entwurf das Prinzip der Datenvermeidung aus dem Text gestrichen hat – ein fatales Zeichen zugunsten einer noch weiter ausufernden Verarbeitung personenbezogener Daten.

Die Konferenz spricht sich für eine ausdrückliche Verankerung des Prinzips der Datensparsamkeit in Art. 5(1)(c) DSGVO entsprechend der Formulierung der Kommission bzw. des Parlaments aus.

4. Keine Aufweichung der Zweckbindung!

Die Zweckbindung ist seit jeher eines der zentralen Prinzipien des Datenschutzrechts. Sie dient der Transparenz und Vorhersehbarkeit der Verarbeitung personenbezogener Daten und stärkt damit die Autonomie der Betroffenen. Angesichts der Unsichtbarkeit und des Umfangs der Datenverarbeitung muss sich der Betroffene darauf verlassen können, dass seine personenbezogenen Daten grundsätzlich nur zu den Zwecken weiterverarbeitet werden, zu denen sie erhoben worden sind. Art. 8 Abs. 2 der Europäischen Grundrechtecharta hat daher die Zweckbindung als tragendes Prinzip des Datenschutzes verankert.

Dementsprechend folgt der Kommissionsentwurf der DSGVO grundsätzlich dem hergebrachten Ansatz der Richtlinie 95/46/EG, indem er in Art. 5(1)(b) zunächst festlegt, dass personenbezogene Daten nur für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen.

Die Konzeption der geltenden Richtlinie 95/46/EG ist dadurch geprägt, dass sie eine Verarbeitung personenbezogener Daten zu anderen Zwecken nur zulässt, wenn diese neuen Zwecke mit dem Ursprungszweck vereinbar sind. Weitere Zweckänderungen lässt die Richtlinie nicht zu. Auf dieser Basis ist es in der Regel gelungen, einen starken Schutz des

Rechts auf informationelle Selbstbestimmung in einen angemessenen Ausgleich mit den öffentlichen Datenverarbeitungsinteressen des Staates und den legitimen Interessen der Unternehmen zu bringen.

Hiervon abweichend hat die Kommission in ihrem Vorschlag zu Art. 6(4) DSGVO zusätzlich die Möglichkeit vorgesehen, dass personenbezogene Daten auch zu solchen Zwecken weiterverarbeitet werden dürfen, die mit dem ursprünglichen Verarbeitungszweck nicht vereinbar sind. Der Rat hat diese Ausnahme noch erweitert, indem er solche Zweckänderungen auch bei einem überwiegenden berechtigten Interesse des Verarbeiters zulassen will. Spätestens durch diese Ergänzungen werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

Das Europäische Parlament ist deshalb zu dem bewährten Ansatz der Richtlinie 95/46/EG zurückgekehrt und hat konsequenterweise Art. 6(4) DSGVO gestrichen. Dies entspricht auch einer frühzeitig erhobenen Forderung der Artikel-29-Gruppe der Europäischen Datenschutzbehörden.

Die Gewährleistung einer starken Zweckbindung ist eine unabdingbare Voraussetzung, um dem Einzelnen ein Höchstmaß an Entscheidungsfreiheit und Transparenz zu ermöglichen. Die Konferenz lehnt deshalb die vom Rat vorgeschlagene Aufweichung der Zweckbindung entschieden ab und spricht sich auf der Basis des Ratsvorschlages für eine Streichung des Art. 6(4) DSGVO aus.

5. Keinen datenschutzrechtlichen Freibrief für Statistik, Archive sowie wissenschaftliche und historische Zwecke!

Die Verarbeitung personenbezogener Daten für die im öffentlichen Interesse tätigen Archive, für die Statistik sowie für historische und für Forschungszwecke folgt aufgrund der jeweiligen Eigenarten der genannten Zweckbestimmungen zum Teil besonderen Regelungen. In allen Fällen geht es darum, die Grundrechte auf Datenschutz und Privatsphäre in einen angemessenen Ausgleich zu bringen mit wichtigen – zum Teil ebenfalls grundrechtlich – geschützten Interessen wie der Forschungsfreiheit oder den öffentlichen Interessen an der amtlichen Statistik bzw. der langzeitlichen Verfügbarmachung staatlicher Informationen durch die Archive. Dies wird grundsätzlich auch durch die Datenschutzbeauftragten des Bundes und der Länder anerkannt. Das geltende Datenschutzrecht hat diesen Ausgleich bisher angemessen hergestellt.

Der Rat geht in seinem Entwurf in verschiedener Hinsicht über diesen Ansatz hinaus und privilegiert die genannten Bereiche in unannehmbarer Weise. Einerseits soll eine

Weiterverarbeitung zu den genannten Zwecken gem. Art. 5(1)(b) DSGVO generell immer möglich sein; die Zweckbindung wird insoweit aufgehoben. Andererseits soll Art. 6(2) DSGVO die (Weiter-)Verarbeitung zu den genannten Zwecken ermöglichen, ohne dass es der Rechtsgrundlagen des Art. 6(1) DSGVO bedarf. Dies würde bedeuten, dass eine Verarbeitung zu den genannten Zwecken ohne weitere Rechtsgrundlage – vorbehaltlich mitgliedstaatlicher Sonderbestimmungen in Teilbereichen nach Art. 83 DSGVO – möglich wäre und die Weiterverarbeitung personenbezogener Daten, die ursprünglich zu anderen Zwecken erhoben worden sind, weitgehend schrankenlos möglich wäre.

Hinzu kommt, dass der gegenständliche Anwendungsbereich der Privilegierung zu weit gefasst ist. Einzig für die Archive im öffentlichen Interesse bestehen insofern keine Bedenken, zumal sich zumindest die staatlichen Archive nach Art. 83 DSGVO nach dem meist ausdifferenzierten mitgliedstaatlichen Recht zu richten haben. Bei der Privilegierung der statistischen Zwecke differenziert der Ratsentwurf hingegen nicht nach solchen der amtlichen Statistik und sonstigen statistischen Zwecken. Während für erstere im Rahmen von Art. 83 DSGVO eine Privilegierung nachvollziehbar ist, besteht im Übrigen die Gefahr, dass etwa die Betreiber von sozialen Netzwerken, Suchmaschinen, Analysetools usw. die von ihnen vorgenommene umfassende Profilbildung als statistische Zwecke deklarieren. Vergleichbare Bedenken bestehen auch gegen die Privilegierung der wissenschaftlichen Datenverarbeitung, die vom Rat nicht auf Zwecke der wissenschaftlichen Forschung beschränkt wird, sondern darüber hinausgeht.

Datenschutzrechtliche Grundsätze gelten auch für die Verarbeitung personenbezogener Daten zu Zwecken der öffentlichen Archive, der Statistik sowie für wissenschaftliche und historische Zwecke. Die Konferenz erwartet im Trilog eine differenzierte und ausgewogene Regelung zum Schutze der genannten Interessen, die die Einschränkungen der Grundrechte auf Datenschutz und Privatsphäre auf das unabdingbar Notwendige beschränkt. Jede Verarbeitung zu den genannten Zwecken bedarf einer Rechtsgrundlage im Sinne von Art. 6(1) DSGVO. Art. 6(2) DSGVO ist insofern missverständlich und sollte daher gestrichen werden. Darüber hinaus sollte – vergleichbar mit den Archiven – nur die amtliche Statistik privilegiert werden. Profilbildungen in sozialen Netzwerken, Suchmaschinen, durch den Einsatz von Analysetools usw. dürfen nicht privilegiert werden.

6. Die Einwilligung muss die Datenhoheit des Einzelnen sichern!

Recht auf informationelle Selbstbestimmung bedeutet seit jeher, dass der Einzelne grundsätzlich selbst über Preisgabe und Verwendung seiner personenbezogenen Daten entscheiden darf. Daraus folgt unmittelbar, dass der Einzelne grundsätzlich autonom darüber bestimmen kann, ob er eine Verarbeitung seiner personenbezogenen Daten erlaubt oder nicht. Die Einwilligung ist ein wesentliches Element, um diese Autonomie wirksam zu

sichern. Sie ist deshalb in Art. 8 Abs. 2 der EU-Grundrechtecharta ausdrücklich als Legitimation für die Verarbeitung personenbezogener Daten genannt.

Kommission und Parlament haben sich im Bewusstsein dieser Bedeutung dafür entschieden, dass eine Einwilligung nur dann wirksam sein soll, wenn sie ausdrücklich erfolgt. Nur bei einer ausdrücklichen Willensbekundung kann letztlich der Nachweis erbracht werden, dass sich der Einzelne der Tragweite seiner Entscheidung bewusst wird.

Der Rat verabschiedet sich in seinem Entwurf entgegen der Grundrechtecharta von diesem Grundsatz, indem er bereits eine eindeutige Willensbekundung ausreichen lässt. Damit wird es insbesondere den global agierenden Diensteanbietern ermöglicht, durch die Verwendung pauschaler Datenschutzbestimmungen und datenschutzunfreundlicher Voreinstellungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Als datenschutzgerechte Einwilligung kann nur ein opt-in akzeptiert werden.

Es sollte zudem ein Koppelungsverbot ausdrücklich in den verfügenden Teil der DSGVO aufgenommen werden. Während Kommission und Parlament dieses in Artikel 7(4) DSGVO vorsehen, hat es der Rat gestrichen und erwähnt es lediglich in den Erwägungsgründen (EG 34).

Zur wirksamen Gewährleistung des Rechts auf informationelle Selbstbestimmung unterstützt die Konferenz den Ansatz von Kommission und Parlament, dass eine Einwilligung nur dann die Verarbeitung personenbezogener Daten legitimieren kann, wenn sie ausdrücklich abgegeben wird. In Art. 7 DSGVOsollte darüber hinaus ein Koppelungsverbot ausdrücklich geregelt werden.

7. Rechte der Betroffenen

a. Sicherstellung der Unentgeltlichkeit

Die Entwürfe der Kommission und des Parlaments sehen in Art. 12(4) DSGVO vor, dass Unterrichtungen der Betroffenen und *die auf Antrag ergriffenen Maßnahmen* zur Umsetzung der Betroffenenrechte unentgeltlich sind. Der Entwurf des Rates sieht dagegen vor, dass lediglich die Informationen gemäß Art. 14 und 14a sowie alle *Mitteilungen* gemäß den Artikeln 16 bis 19 und 32 unentgeltlich zur Verfügung gestellt werden. Damit bleibt unklar, ob auch die Umsetzung der Betroffenenrechte selbst unentgeltlich erfolgen muss oder die verantwortlichen Stellen hierfür ggf. eine Gebühr erheben können. Dafür spricht, dass nur das Auskunftsrecht (Art. 15) ausdrückliche Regelungen zur (Un-)Entgeltlichkeit enthält (vgl. Art. 15(1) und (1b)), die übrigen Betroffenenrechte hingegen nicht.

Die Unentgeltlichkeit der Ausübung und Umsetzung der Betroffenenrechte ist unabdingbare Voraussetzung für die effektive Wahrnehmung des Rechts auf informationelle Selbstbestimmung. Gebühren für die Ausübung schrecken die Betroffenen regelmäßig von der Wahrnehmung ihrer Rechte ab.

Die Konferenz spricht sich für eine unmissverständliche Regelung aus, dass die Ausübung der Betroffenenrechte und deren Umsetzung durch die verantwortlichen Stellen unentgeltlich erfolgen müssen.

b. Keine Einschränkung der Betroffenenrechte!

Die Information der Betroffenen (Art. 14, 14a DSGVO) versetzt diese in die Lage, Umfang und Risiko der Datenverarbeitung einzuschätzen. Sie ist die wesentliche Bedingung für die Schaffung von Transparenz. Der Entwurf des Rates sieht lediglich die Unterrichtung über die Identität der verantwortlichen Stelle, die Zwecke der Datenverarbeitung und die Rechtsgrundlage vor. Weitergehende Informationen sollen nur dann erforderlich sein, wenn sie unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten.

Die Konferenz lehnt Beschränkungen der Betroffenenrechte ab. Die Formulierungen des Rates führen zu Rechtsunsicherheit und lassen Raum für Interpretationen, die zu einer Absenkung des geltenden Datenschutzniveaus führen.

Die Informationspflichten der Art. 14 und 14a DSGVO beinhalten im Gegensatz zum Recht auf Auskunft (Art. 15) lediglich allgemeine, abstrakte Informationen über Art, Umfang und Zweck der Datenverarbeitung. Die Informationspflicht führt daher nicht zu exzessiven Bürokratiekosten, weil sie in standardisierter Form gegenüber den Betroffenen erfüllt werden kann. Die vom Europäischen Parlament vorgeschlagenen standardisierten Informationsmaßnahmen unter ergänzender Verwendung von Piktogrammen (Art. 13a) erachtet die Konferenz für erwägenswert.

Die Konferenz spricht sich gegen Einschränkungen der Betroffenenrechte aus und unterstützt die Position des Europäischen Parlaments.

c. Wirksame Begrenzung der Profilbildung sicherstellen!

Die Datenschutzbeauftragten des Bundes und der Länder sind der Auffassung, dass die bisherigen Vorschläge für eine Regelung von Profilbildungen in Art. 20 DSGVO nicht geeignet sind, um die Bürgerinnen und Bürger im Zeitalter von Big Data, der Allgegenwart des

Internets der Dinge und der in alle Lebens-, Privat- und Intimbereiche wie die Gesundheit vordringenden Technologien zur individuellen Datenerfassung und -analyse effektiv vor der Erstellung und Nutzung von Persönlichkeitsprofilen zu schützen.

Die Vorschläge von Kommission, Parlament und Rat zu Art. 20 DSGVO sind unzureichend, da keiner der Vorschläge die Profilbildung an sich besonderen Zulässigkeitsvoraussetzungen unterwirft, sondern erst das Treffen einer „automatisierten Entscheidung“ (Rat) oder einer „Maßnahme“ (KOM) auf Basis des Profilings bzw. „Profiling, das Maßnahmen zur Folge hat, die rechtliche oder ähnlich erhebliche Auswirkungen auf die Interessen der betroffenen Person hat“ (EP).

Unzulänglich ist insbesondere der Vorschlag des Rates, da er das Phänomen des Profilings in Anlehnung an Art. 15 Abs. 1 der EG-Datenschutzrichtlinie 95/46 auf das Treffen automatisierter Entscheidungen mit Rechtswirkung für den Einzelnen reduziert. Geregelt wird damit lediglich eine spezifische Folge der Datenverarbeitung im Zusammenhang mit der Auswertung von Persönlichkeitsmerkmalen, nicht aber die grundlegende Frage, zu welchen Zwecken und innerhalb welcher Grenzen Persönlichkeitsprofile überhaupt erstellt und genutzt werden dürfen. Zudem beinhaltet dieser Ansatz in der Praxis ein erhebliches Interpretations- und Umgehungspotenzial im Hinblick auf Dienste oder Anwendungen, die keine unmittelbaren Rechtswirkungen gegenüber dem Betroffenen entfalten, wie die Analyse des Nutzerverhaltens im Internet, die Analyse persönlicher Vorlieben durch ein soziales Netzwerk, die Analyse von Bewegungsdaten oder die Analyse der Körperaktivität mittels Apps und Sensoren.

Vor diesem Hintergrund plädieren die Datenschutzbeauftragten des Bundes und der Länder für eine differenzierte Regelung der Profilbildung und -nutzung in der DSGVO, die folgende Kernelemente beinhalten sollte:

- Statt der Verkürzung auf automatisierte Einzelfallentscheidungen ist ein Ansatz zu wählen, der sämtliche Profilbildungen oder darauf basierende Maßnahmen erfasst. Diesem Ansatz entspricht am ehesten der vom Europäischen Parlament zu Artikel 20 unterbreitete Regelungsvorschlag.

- Ausnahmen vom Verbot der Profilbildung bedürfen eng begrenzter klarer Erlaubnistatbestände. Wegen ihrer hohen Sensitivität sollte zudem festgelegt werden, dass besondere Kategorien personenbezogener Daten nicht in eine Profilbildung einfließen dürfen.

- In jedem Fall sollte die Verarbeitung personenbezogener Daten zu Zwecken des Profilings stets mit einem Höchstmaß an Transparenz und Informiertheit des Betroffenen einhergehen. Der Einzelne muss wissen, wann, zu welchem Zweck und in welcher Form seine Daten im Internet oder bei der Nutzung eines Dienstes auf einem

Endgerät zu Profilingzwecken verarbeitet werden und muss hierzu seine ausdrückliche Einwilligung erteilen.

- Zudem sollte eine Verpflichtung zu frühestmöglicher Anonymisierung oder Pseudonymisierung der für die Profilbildung und -auswertung verwendeten Daten bestehen, letzteres flankiert von einem Verbot der (Re-)Identifizierung.

In Anbetracht der wiederholt vom EuGH festgestellten Gefahren, die von Persönlichkeitsprofilen für das Grundrecht auf Datenschutz ausgehen, fordert die Konferenz, die vorliegenden Vorschläge für eine Profilingregelung im Sinne der vorgenannten Eckpunkte substanziell zu verbessern.

8. Die datenschutzrechtliche Verantwortlichkeit gilt für jede Verarbeitung personenbezogener Daten!

Die in Kapitel IV, insbesondere in Art. 22 DSGVO geregelte Verantwortlichkeit für die Einhaltung der datenschutzrechtlichen Bestimmungen *(Accountability)* gehört zu den zentralen Grundprinzipien eines modernen Datenschutzrechts. Die für die Verarbeitung Verantwortlichen und die Auftragsdatenverarbeiter sind in jedem Falle und ohne Einschränkungen für die Einhaltung des Datenschutzrechts verantwortlich. Dies gilt ungeachtet der Art, des Umfangs, der Umstände und der Zweck der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken für die Betroffenen. Ebenso müssen die für die Verarbeitung Verantwortlichen und Auftragsdatenverarbeiter uneingeschränkt in der Lage sein, die Einhaltung ihrer Pflichten nachzuweisen. Risikobasierte Aspekte dürfen lediglich bei der Frage berücksichtigt werden, welche konkreten Maßnahmen zur Einhaltung der Pflichten zu treffen sind.

Es muss daher klargestellt werden, dass sich ein risikobasierter Ansatz nicht auf das „Ob“ und die Nachweisbarkeit, sondern allenfalls auf das „Wie“ der Einhaltung der Pflichten beziehen kann. Dies wird im Vorschlag der Kommission am besten verdeutlicht, in dem auf jede Relativierung verzichtet wird.

Die Konferenz spricht sich für den seitens der Kommission für Art. 22 DSGVO gewählten Ansatz aus, um zu verdeutlichen, dass die Verantwortlichkeit *(„Accountability“)* ein tragendes Grundelement des Datenschutzes ist, das als solches einem risikobasierten Ansatz nicht zugänglich ist.

9. Für die Verankerung von Gewährleistungszielen beim technischen und organisatorischen Datenschutz!

Die Verarbeitung personenbezogener Daten bedarf zum Schutz der Grundrechte nicht nur eines rechtlichen, sondern auch eines technischen und organisatorischen Schutzes. Ein modernes Datenschutzrecht muss hierfür Gewährleistungsziele definieren, an denen sich die zu treffenden Maßnahmen auszurichten haben. Dies bedeutet, dass zu den klassischen Gewährleistungszielen der IT-Sicherheit spezifische Ziele hinzutreten müssen, die sich namentlich auf den Schutz personenbezogener Daten beziehen. Deshalb sind die Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit, aber auch Nicht-Verkettbarkeit, Transparenz und Intervenierbarkeit in der DSGVO zu verankern. Während sich Kommission und Rat in ihren Vorschlägen zu Art. 30(2) bzw. 30(1a) DSGVO im Wesentlichen auf die klassischen Ziele Verfügbarkeit, Integrität und Vertraulichkeit fokussieren, geht der Ansatz des Parlaments in Art. 30(1a) und 30(2) DSGVO i. V. m. Art. 5(1)(ea) und (eb) am weitesten.

Die Konferenz hält eine konsequente, klare und übersichtliche Verankerung der Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit, Nicht-Verkettbarkeit, Transparenz und Intervenierbarkeit in Art. 30 DSGVO für notwendig. Sie unterstützt insoweit die Zielrichtung des Parlaments, spricht sich allerdings für eine übersichtlichere Gestaltung aus.

10. Guter Datenschutz braucht betriebliche und behördliche Datenschutzbeauftragte!

Ungeachtet der materiell-rechtlichen Bestimmungen hängt das konkrete Datenschutzniveau in Behörden und Unternehmen ganz entscheidend davon ab, welche Akzeptanz der Datenschutz vor Ort genießt und wie die Datenschutzkultur ausgeprägt ist. Hierzu können die Aufsichtsbehörden für den Datenschutz Impulse liefern und durch Kontrollen und Beratungen einen entscheidenden Beitrag leisten. Diese Aktivitäten bleiben aber notwendigerweise punktuell und sind aufgrund der unterschiedlichen Rollen nicht immer konfliktfrei. Deshalb kommt der Institution der Datenschutzbeauftragten in Unternehmen und Verwaltungen eine hohe Bedeutung zu.

Es ist deshalb erfreulich, dass sowohl Kommission als auch Parlament in Art. 35 DSGVO die verpflichtende Bestellung interner Datenschutzbeauftragter vorsehen. Allerdings sind die von beiden Institutionen gewählten Kriterien, unter denen eine Bestellung verpflichtend ist, wenig überzeugend.

Bedauerlicherweise hat sich im Rat eine europaweit geltende Verpflichtung zur Bestellung von Datenschutzbeauftragten nicht durchgesetzt. Hierbei wird vor allem mit dem bürokratischen und wirtschaftlichen Aufwand argumentiert. Nach den jahrzehntelangen Erfahrungen in Deutschland überzeugt dieses Argument nicht. Der Compliance-Aufwand für die Unternehmen ist ohne die Einbindung betrieblicher Datenschutzbeauftragter nicht

unerheblich; durch deren Einsatz können zudem Sanktionen und Bußgelder oftmals vermieden werden.

Die Konferenz setzt sich nach wie vor dafür ein, dass eine verpflichtende Bestellung betrieblicher und behördlicher Datenschutzbeauftragter europaweit verbindlich vorgeschrieben wird. Während es für Behörden keine Ausnahmen geben sollte, sollten Unternehmen nicht nur ab einer bestimmten Größe oder einer bestimmten Zahl Betroffener einen Datenschutzbeauftragten bestellen, sondern in jedem Falle auch dann, wenn die Datenverarbeitung mit besonderen Risiken für die Rechte und Freiheiten der Betroffenen verbunden ist.

11. Mehr Kontrolle über Datenübermittlungen an Behörden und Gerichte in Drittstaaten!

Seit den Enthüllungen von Edward Snowden wird intensiv über einen besseren Schutz der personenbezogenen Daten von europäischen Bürgerinnen und Bürgern gegenüber Behörden und Stellen aus Drittstaaten diskutiert. Deshalb hat das Parlament einen spezifischen Art. 43a DSGVO vorgeschlagen. Dieser stellt klar, dass Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaats, die von einem für die Verarbeitung Verantwortlichen die Weitergabe personenbezogener Daten verlangen, in der EU grundsätzlich weder anerkannt werden noch vollstreckbar sind, wenn dies nicht in internationalen Übereinkommen zur Amts- oder Rechtshilfe festgelegt ist. Sie stehen dann im Einzelfall unter dem Genehmigungsvorbehalt der in den Abkommen bezeichneten zuständigen Stellen.

Die Konferenz unterstützt diese Forderung ebenso wie die Artikel-29-Gruppe. Mit der Schaffung einer solchen Regelung wird die Tätigkeit ausländischer Nachrichtendienste in Europa zwar nicht unterbunden. Sie könnte jedoch in einem gewissen Umfang Transparenz über das Ausmaß der Überwachung herstellen, zur Wahrung der Verhältnismäßigkeit beitragen und vor allem Anreize zur Verabschiedung internationaler Übereinkommen schaffen.

Der Rat ist einer entsprechenden Initiative der Bundesregierung bedauerlicherweise nicht gefolgt.

Die Konferenz spricht sich weiterhin dafür aus, eine spezifische Rechtsgrundlage für die Datenübermittlung an Behörden und Gerichte in Drittstaaten zu schaffen, mit der insbesondere im Hinblick auf die nachrichtendienstliche Überwachung mehr Transparenz und Kontrolle geschaffen wird. Sie unterstützt den vom Parlament eingebrachten Vorschlag eines Art. 43a DSGVO.

Die Zuständigkeit sollte jedoch wie folgt geregelt werden: Haben ersuchender und ersuchter Staat ein Rechtshilfeabkommen oder einen ähnlichen internationalen Vertrag geschlossen, sollte die hierin bezeichnete Stelle für die Entgegennahme und Prüfung eines Ersuchens auf Datenübermittlung zuständig sein. In den Fällen, in denen eine zuständige Stelle nicht vertraglich bestimmt worden ist, kann diese Aufgabe nachrangig in die Zuständigkeit der Datenschutzaufsichtsbehörden fallen.

12. Für eine effektive und bürgernahe Zusammenarbeit der Datenschutzbehörden in Europa

Ein entscheidender Fortschritt der Datenschutz-Grundverordnung soll in einer verbesserten Zusammenarbeit der Datenschutzbehörden in Europa liegen. Um dies zu gewährleisten und auf der anderen Seite den Unternehmen einen Mehrwert zu bieten, hatte die Kommission einen sog. One-Stop-Shop, einen Kohärenzmechanismus und die Einrichtung eines Europäischen Datenschutzausschusses vorgeschlagen.

Auf Vorschlag des Rats soll es eine federführende Datenschutzbehörde geben, die einem Unternehmen am Ort seiner Hauptniederlassung als hauptsächlicher Ansprechpartner zur Verfügung steht, aber auch mit allen anderen – sei es aufgrund weiterer Niederlassungen oder der Betroffenheit ihrer Bürger – betroffenen Aufsichtsbehörden kooperiert. Weiterhin hat der Rat Vorschläge zu einem sog. One-Stop-Shop gemacht, sodass Betroffene sich an die Aufsichtsbehörde und die Gerichte bei ihnen vor Ort wenden können. Um zu verbindlichen Entscheidungen ohne Beteiligung der Kommission zu kommen, schlägt der Rat darüber hinaus vor, den Europäischen Datenschutzausschuss mit verbindlichen Entscheidungsbefugnissen auszustatten. Hierzu ist der Ausschuss mit eigener Rechtspersönlichkeit auszustatten. Das vom Rat vorgeschlagene Modell ist für die Aufsichtsbehörden komplex, soll aber den Bürgerinnen und Bürgern eine ortsnahe Bearbeitung ihrer Anliegen und den Unternehmen einen Ansprechpartner für länderübergreifende Datenverarbeitungen verschaffen.

Die Konferenz unterstützt die Ziele des Ratsvorschlags zum sog. One-Stop-Mechanismus. Der effiziente Vollzug des Datenschutzrechts darf jedoch nicht durch die Untätigkeit der federführenden Datenschutzbehörde unterlaufen werden. Es ist eine Regelung zu schaffen, wonach die mitgliedstaatlichen Aufsichtsbehörden bei Betroffenheit ihrer Bürger von der federführenden Behörde ein aufsichtsbehördliches Einschreiten verlangen können, dessen Ablehnung zu einer unmittelbaren Überprüfung durch den Europäischen Datenschutzausschuss führt.

Der One-Stop-Shop soll einen ausgewogenen Ausgleich zwischen den verschiedenen Interessen schaffen, eine bürgernahe Bearbeitung von Beschwerden ermöglichen, den

Unternehmen klare Ansprechpartner zur Verfügung stellen und durch die Aufwertung des Europäischen Datenschutzausschusses die notwendige Verbindlichkeit und damit Rechtssicherheit aufweisen. Die Konferenz bittet die am Trilog beteiligten Parteien gleichwohl, praktikable Verfahrensregeln festzulegen. Dies betrifft insbesondere die Frage der Verfahrensfristen und der Amtshilfe der Aufsichtsbehörden untereinander.

13. Für einen starken Beschäftigtendatenschutz

Die DSGVO überlässt die Regelung des Datenschutzes für Beschäftigte in Artikel 82 dem mitgliedstaatlichen Recht. Der Rat und die Kommission legen fest, dass die Mitgliedstaaten dabei den Rahmen der DSGVO einhalten müssen und verzichten auf konkretere Anforderungen. Das Europäische Parlament gibt dagegen ganz konkrete Mindeststandards im Verordnungstext vor.

Die Konferenz hält es für wichtig, dass Artikel 82 DSGVO den Mitgliedstaaten in jedem Falle die Möglichkeit eröffnet, auch über den Standard der DSGVO hinausgehen zu können. Die Konferenz begrüßt den Ansatz des Parlaments, konkrete Mindeststandards für den Beschäftigtendatenschutz im Verordnungstext selbst vorzusehen.

Im Kontext der Verarbeitung von Beschäftigtendaten sollte es die Datenschutz-Grundverordnung den Mitgliedstaaten ermöglichen, im Sinne einer Mindestharmonisierung auch über das Datenschutzniveau der Verordnung hinauszugehen. Die Konferenz unterstützt den Ansatz des Parlaments, konkrete Mindeststandards festzulegen.