Schriftliche Information gemäß § 6 EU-InfoG

Legislativverfahren:

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)
[Dok 9565/15]

1. Inhalt und Ziel der Vorlage

- Geltende Rechtslage

Das allgemeine europäische Datenschutzrecht ist derzeit sekundärrechtlich im Wesentlichen in der Datenschutz-Richtlinie 95/46/EG (DS-RL) geregelt. Mit dem von der Europäischen Kommission (EK) Ende Jänner 2012 vorgelegten Vorschlag für eine Verordnung des Europäischen Parlaments (EP) und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung, [KOM (2012) 11 endg]) auf der Grundlage des Art. 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ist – erstmals – ein einheitlicher und bedingt durch die gewählte Rechtsaktform der Verordnung gemäß Art. 288 Abs. 2 AEUV in jedem Mitgliedstaat unmittelbar gültiger und anwendbarer Rechtsrahmen im Bereich des allgemeinen Datenschutzes intendiert, der zu einer weitgehenden Harmonisierung in diesem Bereich führen soll. Die angesprochene Datenschutz-Grundverordnung soll auf unionsrechtlicher Ebene die derzeit in Geltung stehende Datenschutz-Richtlinie ersetzen.

- Vorschlag einer Datenschutz-Grundverordnung

Die wichtigsten politischen Ziele der EK bei der Vorstellung des Vorschlages waren:

- Modernisierung des EU-Rechtsrahmens zum Schutz personenbezogener Daten, insbesondere um den Herausforderungen der Globalisierung und der Nutzung neuer Technologien gerecht zu werden;
- Stärkung der Betroffenenrechte und gleichzeitiges Abbauen von Verwaltungsformalitäten, um den freien Verkehr personenbezogener Daten innerhalb der EU und darüber hinaus zu gewährleisten;
- Stärkere Harmonisierung der EU-Vorschriften zum Schutz personenbezogener Daten und wirksame Umsetzung und Anwendung des Grundrechts auf Schutz der persönlichen Daten in allen Tätigkeitsbereichen der Union.

Da es sich um einen äußerst umfangreichen Vorschlag handelt, werden nachstehend bestimmte Bereiche von besonderer Bedeutung herausgegriffen.

Allgemeine Bestimmungen (Kapitel I)

In diesem Kapitel werden allgemeine Bestimmungen wie der Gegenstand und die Zielsetzung der Verordnung festgelegt. Weiters werden der sachliche und räumliche Anwendungsbereich sowie Begriffsbestimmungen festgelegt.

Grundprinzipien der rechtmäßigen Datenverwendung (Kapitel II)

Kapitel II regelt im Wesentlichen die elementaren Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5) unter besonderer Bezugnahme auf die Kriterien für eine rechtmäßige Datenverarbeitung (Art. 6). Näher geregelt wird auch, unter welchen Voraussetzungen eine Zustimmung eine rechtswirksame Grundlage für eine rechtmäßige Verarbeitung personenbezogener Daten darstellen kann (Art. 7). Weiters werden in Art. 8 Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten von Kindern im Zusammenhang mit Diensten der Informationsgesellschaft, die Kindern direkt angeboten werden, festgelegt. Dieses Kapitel enthält auch das allgemeine Verbot für die Verarbeitung besonderer Kategorien personenbezogener Daten (sog. sensible Daten), sowie die Ausnahmen von diesem Verbot (Art. 9). Art. 10 stellt schließlich klar, dass ein Auftraggeber allein zur Einhaltung einer Vorschrift dieser Verordnung keine zusätzlichen Informationen einholen muss, um die betroffene Person zu identifizieren

Rechte der betroffenen Personen (Kapitel III)

In diesem Kapitel werden unter anderem Verpflichtungen zur Bereitstellung transparenter, leicht zugänglicher und verständlicher Informationen festgelegt. Weiters wird das Recht der betroffenen Person auf Auskunft über die zu ihr verarbeiteten personenbezogenen Daten (Art. 15) und das Recht auf Richtigstellung (Berichtigung; Art. 16) festgelegt. Art. 17 garantiert dem Betroffenen das Recht, vergessen zu werden, sowie das Recht auf Löschung. In Art. 18 wird das Recht des Betroffenen auf Datenportabilität eingeführt, d.h. das Recht, seine Daten aus einem automatisierten Datenverarbeitungssystem auf ein anderes System zu übertragen. Art. 19 gewährleistet das Widerspruchsrecht der betroffenen Person und Art. 20 enthält Regelungen zur automatisierten Generierung von Einzelentscheidungen (im engeren Sinne: Profiling). Art. 21 ermächtigt den Unionsgesetzgeber und die Mitgliedstaaten unter bestimmten Voraussetzungen,

die Pflichten und Rechte aus der Datenschutz-Grundverordnung sowie die Grundsätze nach Art. 5 zu beschränken.

Für die Verarbeitung Verantwortlicher („Auftraggeber“) und Auftragsverarbeiter („Dienstleister“; Kapitel IV)

Kapitel IV der Datenschutz-Grundverordnung regelt die Rechte und Pflichten des für die Verarbeitung Verantwortlichen („Auftraggeber“) und des Auftragsverarbeiters („Dienstleister“). Weiters finden sich in diesem Kapitel Regelungen zur Datensicherheit, zur Datenschutz-Folgenabschätzung, zur Konsultation der Aufsichtsbehörde und zum Datenschutzbeauftragten.

Regelung des internationalen Datentransfers (Kapitel V)

Kapitel V der Datenschutz-Grundverordnung regelt die näheren Details der Zulässigkeit der Datenübermittlung an Drittstaaten. Dieses Kapitel legt somit die Voraussetzungen für die Datenübermittlung in einen Drittstaat (dh: nicht EU/EWR) fest. Grundsätzlich sind Datentransfers in Drittstaaten demnach nur zulässig, wenn das Recht natürlicher Personen auf ein hohes Datenschutzniveau gewährleistet ist.

Eine genehmigungsfreie Übermittlung in einen Staat außerhalb der EU/des EWR ist nach Kapitel V der Datenschutz-Grundverordnung zunächst dann zulässig, wenn eine Entscheidung der Kommission gemäß Art. 41 des Verordnungsvorschlags vorliegt, die die Angemessenheit des Datenschutzniveaus in diesem Drittstaat bestätigt (sogenannte „Angemessenheitsentscheidung“ oder „Adäquanzentscheidung“). Weiters kann die Übermittlung in einen Drittstaat genehmigungsfrei erfolgen, wenn „geeignete Garantien“ gemäß Art. 42 vorliegen. Dies wäre etwa der Fall, wenn sich das Unternehmen verbindlichen unternehmensinternen Vorschriften unterwirft („Binding Corporate Rules“ – BCR; Art. 43 des Verordnungsvorschlags) oder bei der Verwendung von Standardvertragsklauseln. Auch Verhaltenskodizes und Zertifizierungen wurden als weitere Möglichkeiten für geeignete Garantien in den Verordnungstext aufgenommen.

In Art. 44 des Verordnungsvorschlags sind schließlich Ausnahmebestimmungen für spezielle Fälle von Datentransfers in ein Drittland vorgesehen: Zulässig ist der Datentransfer in einen Drittstaat ohne Genehmigung der Aufsichtsbehörde demnach ausnahmsweise etwa auch dann, wenn der Betroffene der Übermittlung ausdrücklich zugestimmt hat, nachdem er über die Risiken einer Übermittlung ohne Angemessenheits-

entscheidung der Kommission und ohne Vorliegen geeigneter Garantien aufgeklärt wurde. Weitere Ausnahmen bestehen, wenn eine Übermittlung zum Schutz lebenswichtiger Interessen oder zur Wahrung eines wichtigen öffentlichen Interesses erforderlich ist, wie zum Beispiel für den internationalen Datenaustausch zwischen Wettbewerbsbehörden, Steuer- oder Zollverwaltungen oder zwischen Diensten, die für Angelegenheiten der sozialen Sicherheit zuständig sind. Auch die Datenübermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen fällt unter die Ausnahmebestimmung des Art. 44 der Datenschutz-Grundverordnung. Gegenüber der Datenschutz-Richtlinie 95/46/EG neu hinzugekommen ist die Ausnahmebestimmung einer Datenübermittlung in einen Drittstaat bei Vorliegen eines „berechtigten Interesses“ des Auftraggebers.

Prinzip einer einheitlichen Kontaktstelle – One-Stop-Shop (Kapitel VI und VII)

Schon der Vorschlag der EK sieht als Grundgedanken die Einrichtung einer zentralen Kontaktstelle für den Datenschutz in der EU vor: Der Auftraggeber soll sich nur mehr an eine Datenschutzbehörde wenden müssen und zwar an die Datenschutzbehörde des Mitgliedstaats, in dem sich die Hauptniederlassung oder die einzige Niederlassung des Unternehmens befindet (siehe Art. 51a – Zuständigkeit der federführenden Aufsichtsbehörde). Hauptkritikpunkt an dem von der EK vorgeschlagenen Modell war die fehlende Bürgernähe. Das System wurde daher in der weiteren Diskussion umgestaltet, um diese (besser) zu gewährleisten:

Findet die Verarbeitung personenbezogener Daten im Zusammenhang mit der Tätigkeit einer Niederlassung eines Auftraggebers oder eines Dienstleisters in der Union statt und hat dieser Niederlassungen in mehr als einem Mitgliedstaat oder hat die Verarbeitungstätigkeit im Zusammenhang mit der Tätigkeit einer einzigen Niederlassung eines Auftraggebers (oder Dienstleisters) in der Union erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat bzw. wird sie voraussichtlich solche Auswirkungen haben, so soll die Aufsichtsbehörde des Mitgliedstaats für die Hauptniederlassung oder für die einzige Niederlassung als federführende Aufsichtsbehörde fungieren.

Eine wesentliche Neuerung gegenüber dem ursprünglichen Kommissionsvorschlag ist nunmehr die Einbindung der anderen betroffenen Aufsichtsbehörden. Dies sind die Behörden jener Mitgliedstaaten, in denen sich ebenfalls Niederlassungen eines Auftrag-

gebers befinden oder in denen Personen durch die Datenverarbeitung substantiell betroffen sind (zB durch Einbringung einer Beschwerde). Je nach Art der Datenverarbeitung kann dies im weitesten Sinn alle oder allenfalls auch nur einige wenige Datenschutzbehörden betreffen. Das dafür geschaffene Mitentscheidungsverfahren nach Art. 54a sieht vor, dass die federführende Aufsichtsbehörde gemeinsam mit den sonstigen betroffenen Behörden eine Einigung über die zu treffende Entscheidung erzielt. Art. 54a trifft auch umfassende Vorkehrungen hinsichtlich der Annahme der gemeinsamen Entscheidungen durch diese Behörden im Zusammenhang mit Beschwerden von betroffenen Personen, um die gerichtliche Überprüfbarkeit für den Bürger zu erleichtern.

Falls eine dieser sonstigen betroffenen Behörden einen „relevanten und begründeten Einspruch“ gegen den Entscheidungsentwurf der federführenden Aufsichtsbehörde erhebt, wird ein umfassender Streitbeilegungsmechanismus über den Europäischen Datenschutzausschuss (EDPB – European Data Protection Board) vorgesehen (Art. 57 – Kohärenzverfahren). In diesem Fall ist die Entscheidung des EDPB bindend (vgl. Art. 57 Abs. 3).

Neu eingeführt wurden auch sog. „lokale Fälle“, in denen zwar eine Hauptniederlassung besteht, die jedoch konkret nur die Niederlassung in einem Mitgliedstaat betreffen bzw. nur Personen in einem Mitgliedstaat substantiell berühren (siehe Art. 51a Abs. 2a bis 2d). Diese Fälle sollen vorrangig durch die lokale Datenschutzbehörde (DPA) behandelt werden. Die Details diesbezüglich waren Gegenstand umfassender Diskussionen.

2. Stand des Verfahrens auf europäischer Ebene

Am 15./16. Juni 2015 konnte der Rat Justiz und Inneres mehrheitlich eine allgemeine Ausrichtung über die gesamte Datenschutz-Grundverordnung erreichen (Dok 9565/15). Die Trilogverhandlungen mit dem Europäischen Parlament haben noch unter lettischer Präsidentschaft am 24. Juni 2015 begonnen und werden nunmehr unter luxemburgischem Vorsitz intensiv fortgesetzt.

Die erste Trilog-Verhandlungsrunde unter luxemburgischem Vorsitz am 14. Juli 2015 war dem Kapitel V (internationaler Datenverkehr) gewidmet. Am 16./17. September 2015 findet die nächste Trilog-Verhandlungsrunde zu Kapitel II (Grundprinzipien) und Kapitel III (Betroffenenrechte) statt. Das politische Ziel, die Verhandlungen über die Da-

tenschutz-Grundverordnung bis zum Ende des Jahres 2015 abzuschließen, ist nach wie vor aufrecht.

Das Europäische Parlament hat seine Position zur Datenschutz-Grundverordnung am 12. März 2014 beschlossen. Der Europäische Rat hat im Oktober 2013 einen Abschluss der Verhandlungen über den neuen Rechtsrahmen für das Jahr 2015 gefordert. Eine ähnliche Formulierung findet sich auch in den Schlussfolgerungen des Europäischen Rates vom 26./27. Juni 2014 sowie vom 25./26. Juni 2015.

- Österreichische Position

Aus österreichischer Sicht war in den bisherigen Verhandlungen stets wesentlich, dass das derzeit durch das DSG 2000 gewährleistete – und inhaltlich durch die Datenschutz-Richtlinie determinierte – Datenschutzniveau auch im Falle der Erlassung der Datenschutz-Grundverordnung erhalten bleibt und keine Verschlechterung beim Schutz personenbezogener Daten für die Betroffenen eintritt.

Da die Datenschutz-Grundverordnung in der Fassung der allgemeinen Ausrichtung diese Vorgabe aus österreichsicher Sicht nicht in allen Belangen zweifelsfrei erfüllt, hat Österreich der allgemeinen Ausrichtung zur Datenschutz-Grundverordnung am JI-Rat am 15./16. Juni 2015 nicht zugestimmt. Die wesentlichen Bedenken im Einzelnen wurden in einer Erklärung zum Ratsprotokoll dargelegt.

Nach österreichischer Auffassung schwächt die derzeit vorliegende Textfassung den ursprünglichen Kommissionsvorschlag in einzelnen Punkten aus datenschutzrechtlicher Sicht deutlich ab (zB Beseitigung des klaren Grundsatzes der Datensparsamkeit aus dem Kommissionsvorschlag: Streichung von „limited to the minimum necessary“ zugunsten einer Regelung, wonach die Datenverwendung nur „not excessive“ sein darf). In anderen Punkten unterschreitet die vorliegende Textfassung für die allgemeine Ausrichtung das Datenschutzniveau der derzeit geltenden Datenschutz-Richtlinie (zB wäre nunmehr eine Auslandsdatenübermittlung auch ausschließlich aufgrund des berechtigten Interesses des Auftraggebers möglich; die Datenschutz-Richtlinie sieht eine derartige Ausnahme nicht vor). Zudem würde die derzeitige Textfassung dazu führen, dass nationale Schutzgesetze zugunsten Privater (zB Regelungen zur privaten Videoüberwachung) mangels einer eindeutigen Ermächtigung, derartige Regelungen auch nach

dem Inkrafttreten der Datenschutz-Grundverordnung aufrechterhalten zu dürfen, wegfallen. Dies steht nach österreichischer Auffassung auch in einem Spannungsverhältnis zu den Verpflichtungen der Staaten aus Art. 8 EMRK, nationale Gesetze zum Schutz der Grundrechtsträger zu erlassen. Nicht zuletzt hält es Österreich für erforderlich, dass den Mitgliedstaaten ausdrücklich die Möglichkeit gegeben wird, im Kontext des Arbeitnehmerdatenschutzes strengere nationale Regelungen vorzusehen.

Im Detail darf zu einzelnen dargelegten Punkten auf die nachfolgenden Ausführungen verwiesen werden:

Kapitel I – Allgemeine Bestimmungen

Zur Thematik spezifischerer Regelungen für private Datenanwendungen im nationalen Recht

Auf Wunsch zahlreicher Mitgliedstaaten wurde in Art. 1 Abs. 2a eine Regelung für den öffentlichen Sektor aufgenommen, die es den Mitgliedstaaten ermöglicht, nationale spezifischere Regelungen für diesen Bereich zu verabschieden („Flexibilisierungsklausel“). Die Regelung greift aus österreichischer Sicht jedoch zu kurz, da die Mitgliedstaaten auch in Bezug auf private Datenanwendungen spezifischere Regelungen zum Schutz Betroffener aufrechterhalten bzw. erlassen können müssen (zB Regelungen zur Videoüberwachung im privaten Bereich nach § 50a Datenschutzgesetz 2000 – DSG 2000).

Art. 1 der Verordnung hätte daher von Österreich grundsätzlich akzeptiert werden können, wenn an anderer Stelle den Mitgliedstaaten zusätzlich auch Flexibilität für den privaten Bereich eingeräumt worden wäre. Anstelle einer solchen Ergänzung (im verfügenden Teil) wurde nur eine interpretative Ergänzung in EG 8 aufgenommen, die bewirken soll, dass die Flexibilisierungsbestimmung für den öffentlichen Sektor in Art. 1 Abs. 2a iVm Art. 6 Abs. 3 der Verordnung auch für den privaten Bereich gilt. Diese Lesart hält aber einer kritischen Prüfung nicht stand. Österreich bestand zudem iSd der Rechtsklarheit und -sicherheit auf einer eindeutigen Verankerung im verfügenden Teil der Verordnung.

Zu Art. 2 lit. d und EG 15 – „Haushaltsausnahme“

Gerade die leichte technische Möglichkeit zur Verbreitung von Daten etwa über soziale Medien erfordert nach österreichischer Auffassung eine Einbeziehung vordergründig rein privater Aktivitäten auf diesem Felde zumindest in den Geltungsbereich der Daten-

schutzgrundsätze und Individualrechte, uzw. jedenfalls dann, wenn Dritte betroffen sind (Bsp.: Upload von Gruppenfotos).

Im derzeit geltenden Unionsrecht findet sich die sog. Haushaltsausnahme in Art. 3 Abs. 2 der DS-RL 95/46/EG. Innerstaatlich regelt § 45 DSG 2000 die Verarbeitung personenbezogener Daten zu privaten Zwecken. Demnach dürfen natürliche Personen Daten für ausschließlich persönliche oder familiäre Tätigkeiten verarbeiten, wenn sie ihnen vom Betroffenen selbst mitgeteilt wurden oder ihnen sonst rechtmäßigerweise […] zugekommen sind. Das in Umsetzung der Datenschutz-Richtlinie erlassene DSG 2000 nimmt somit diese Art der Datenverwendung nicht pauschal aus seinem Geltungsbereich aus, sondern schafft einen spezifischen Erlaubnistatbestand. Zugleich wird eine strikte Zweckbindung bzw. ein Weiterverwendungsverbot für andere Zwecke statuiert (vgl. § 45 Abs. 2 DSG 2000). Die vom Vorsitz vorgeschlagene Ausnahme vom Anwendungsbereich im Lichte der Auslegung im EG 15 kann daher von Österreich nicht unterstützt werden und würde einen klaren Rückschritt hinsichtlich der geltenden Rechtslage bedeuten.

Kapitel II – allgemeine Grundprinzipien

Hinsichtlich des Kapitels II konnte Österreich bereits beim JI-Rat am 12./13. März 2015 der partiellen allgemeinen Ausrichtung zu diesem Kapitel der Datenschutz-Grundverordnung nicht zustimmen und hat in einer Erklärung zum Ratsprotokoll die vorhandenen Bedenken dargelegt.

Zur österreichischen Position zu Kapitel II ist im Detail auf die nachfolgende Auflistung zu verweisen. Dabei handelt es sich um eine beispielhafte Aufzählung der georteten Problembereiche. Neben der untenstehenden Auflistung besteht beispielsweise auch noch Klärungsbedarf in Art. 8 (Schutz von Kindern), Art. 5 (Grundsatz der Datensparsamkeit) oder bei den pseudonymen Daten (der Schlüssel für die Pseudonymisierung darf niemals in der Ingerenz des Auftraggebers liegen). Österreich hat seine diesbezüglichen Positionen im Dok 6741/15 dargelegt.

Verarbeitung von personenbezogenen Daten auf der Grundlage eines berechtigten Interesses des Auftraggebers (Art. 6 Abs. 1 lit. f und EG 38, 38a, 39 und 40)

Art. 7 lit. f der derzeit in Geltung stehenden Datenschutz-Richtlinie lässt eine Datenverarbeitung auch im Fall einer Interessenabwägung zugunsten des Auftraggebers oder

eines Dritten zu. Wesentlich ist, dass nach der DS-RL schon ein „Gleichstand“ des (relativ leicht befürwortbaren) legitimen Interesses des Auftraggebers im Verhältnis zum Interesse des Betroffenen die Zulässigkeit der Datenverwendung bewirkt. Damit ist die DS-RL bei der Zulässigkeitsprüfung weniger streng als das DSG 2000. § 8 Abs. 1 Z 4 DSG 2000 sieht nämlich vor, dass schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht sensibler personenbezogenen Daten nur nicht verletzt sind, wenn überwiegende berechtigte Interessen des Auftraggebers oder eines Drittens die Verwendung erfordern. Andernfalls ist die Datenverwendung unzulässig. Dieser Unterschied zwischen dem Wortlaut des Art. 7 lit. f DS-RL und jenem von § 8 Abs. 1 Z 4 DSG 2000 ist nicht nur durch das den Mitgliedstaaten in Art. 5 DS-RL eingeräumte Ermessen („Die Mitgliedstaaten bestimmen nach Maßgabe dieses Kapitels die Voraussetzungen näher, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist“) gedeckt, sondern zudem durch das Prinzip einer grundrechtsfreundlichen Auslegung der DS-RL und Rechtssicherheitsüberlegungen geboten.

Österreich hat in den Diskussionen zum Kapitel II wiederholt vorgebracht, dass die textliche Ausgestaltung und Interpretation des berechtigten Interesses des Auftraggebers – vor allem in den zitierten EG – nicht akzeptiert werden kann. Das alleinige Vorliegen eines berechtigten Interesses des Auftraggebers kann – ohne eine verpflichtende Abwägung dieses Interesses mit dem Interesse des Betroffenen auf Geheimhaltung – niemals eine Datenverarbeitung rechtfertigen. Das derzeitige Konzept der Zulassung eines „Gleichstands“ der Interessen begünstigt aber eine solche Handhabung in der Praxis, benachteiligt den Betroffenen in einer solchen Situation, weil es ihm die Beweislast für überwiegende Interessen auf seiner Seite auferlegen könnte und leistet insgesamt der Rechtsunsicherheit Vorschub. Es muss daher darauf abgestellt werden, dass für einen Grundrechtseingriff das Interesse des Auftraggebers an der Datenverarbeitung gegenüber dem Geheimhaltungsinteresse des Betroffenen zu überwiegen hat. Österreich hat diese Überlegungen in einem eigenen Ratsdokument näher ausgeführt (Dok 6741/15). Die in der Textfassung für die allgemeine Ausrichtung des Rates vorgesehene Konstruktion, dass weiterhin nur auf das Vorliegen eines berechtigten Interesses des Auftraggebers abgestellt wird, welches das des Betroffenen nicht überwiegen muss, würde – im Lichte der unmittelbaren Anwendbarkeit ohne Rückgriffsmöglichkeit auf eine dem Art. 5 der DS-RL entsprechende Klausel – insofern zu einer Senkung des Schutzniveaus führen und konnte von Österreich nicht akzeptiert werden.

Weiterverwendung von Daten (Art. 6 Abs. 3a und 4, EG 40)

Art. 6 Abs. 1 lit. b der derzeit in Geltung stehenden Datenschutz-Richtlinie 95/46/EG normiert das zentrale Prinzip der Zweckbindung. Dementsprechend dürfen Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden. Dabei besteht folgende Ausgangslage: Personenbezogene Daten werden originär für einen bestimmten Zweck auf der Basis einer bestehenden Rechtsgrundlage verarbeitet, später jedoch für einen anderen Zweck weiterverarbeitet (Weiterverwendung). Nach österreichischem Verständnis stellt eine Weiterverwendung zu anderen Zwecken eine Datenübermittlung dar, deren Zulässigkeit gesondert zu prüfen ist.

Ausdrücklich geregelt ist in Art. 6 Abs. 2 lit. b der DS-RL, dass die Weiterverwendung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken im allgemeinen nicht als unvereinbar mit den Zwecken der vorangegangenen Datenerhebung anzusehen ist, sofern die Mitgliedstaaten geeignete Garantien vorsehen (siehe §§ 46 und 47 DSG 2000). Grundsätzlich stellt sich in diesem Zusammenhang jedoch allgemein die Frage, ob das Zweckbindungsprinzip, wonach die Daten nicht in einer mit dem ursprünglichen Zweck unvereinbaren Weise weiterverwendet werden dürfen, nicht in den meisten Fällen einer derartigen Weiterverwendung entgegensteht. Gemeint ist damit die Frage nach der Bedeutung des Inkompatibilitätsgebots für die Weiterverwendung von Daten, welche bis dato auf europäischer Ebene nicht eindeutig geklärt wurde.

Der Vorschlag der Datenschutz-Grundverordnung versucht dies einer Lösung zuzuführen: Art. 6 Abs. 3a und 4 normiert die Rechtmäßigkeit der Weiterverwendung von personenbezogenen Daten. In der bisherigen Diskussion bestand große Unklarheit hinsichtlich der Frage, ob für die Verwendung von Daten für einen weiteren Zweck nur dann eine – für diese Weiterverarbeitung gesonderte – Rechtsgrundlage erforderlich ist, wenn dieser weitere Zweck mit dem originären Zweck für die Datenverarbeitung unvereinbar ist (inkompatibler Zweck), oder eine solche auch bei einem kompatiblen Zweck erforderlich ist. Dies manifestiert sich insbesondere im Zusammenhang mit Verarbeitungen zu Archivzwecken, statistischen, historischen und wissenschaftlichen Zwecken.

Österreich hat bisher die Versuche, eine Lösung für diesen Themenbereich zu finden, stets unterstützt und daher auch im Dok. 6741/15 bzw. 8408/15 umfassend Stellung

bezogen und konkrete Vorschläge unterbreitet. In den Verordnungstext teilweise aufgenommen wurde die Forderung, dass es sich im Rahmen der Weiterverwendung von Daten immer um denselben Auftraggeber handeln muss, da dies – bei Fehlen einer solchen Einschränkung – ansonsten zu einer uferlosen Ermächtigung zur Datenweiterverwendung über den ursprünglichen Auftraggeber hinaus werden würde. Dies muss sowohl für die Weiterverwendung zu kompatiblen als auch inkompatiblen Zwecken gelten. Es fehlt daher dieser Verweis in Art. 6 Abs. 3a des Verordnungsentwurfs.

Problematisch ist insbesondere der letzte Satz des Art. 6 Abs. 4 („Die Weiterverarbeitung durch denselben für die Verarbeitung Verantwortlichen für nicht konforme Zwecke aufgrund der berechtigten Interessen dieses für die Verarbeitung Verantwortlichen oder eines Dritten ist rechtmäßig, wenn diese Interessen die Interessen der betroffenen Person überwiegen."). Aus österreichischer Sicht wird dadurch einer Aushöhlung des Zweckbindungsgrundsatzes Vorschub geleistet bzw. der Interessenabwägung als Rechtsgrundlage im Art. 6 insgesamt ein Verständnis zu Grunde gelegt, das nicht mit Art. 8 der EU-Grundrechte-Charta vereinbar sein könnte.

Zur Möglichkeit der Aufrechterhaltung oder Einführung spezifischerer Regelungen für private Datenanwendungen im nationalen Recht (im Zusammenhang mit Art. 9 Abs. 5 und EG 35a)

Art. 9 Abs. 5 sieht im Bereich der sensiblen Daten (hinsichtlich genetischer Daten und Gesundheitsdaten) die Möglichkeit der Mitgliedstaaten vor, eigene spezifischere nationale Regelungen zu erlassen. Dagegen bestehen aus österreichischer Sicht keine grundsätzlichen Einwendungen. Die Ergänzungen greifen jedoch aus österreichischer Sicht zu kurz, da es einer horizontalen Möglichkeit für die Mitgliedstaaten in der Verordnung bedarf, für spezifische Situationen Regelungen auf nationaler Ebene zum Schutz Betroffener im privaten Bereich beizubehalten oder einzuführen (siehe dazu auch schon die Position Österreichs am JI-Rat im Dezember 2014).

Verweis auf die Rechtmäßigkeit der Verarbeitung im Zusammenhang mit Direktmarketing (EG 39 letzter Satz)

Österreich hat sich bisher immer gegen eine derartige undifferenzierte und absolute Vorabqualifizierung bestimmter Datenverwendungen als „legitimes Interesse" ausgesprochen. Dies ist auch schon deshalb abzulehnen, weil durch die Anknüpfung in der Datenschutz-Grundverordnung an anderen Stellen an das bloße Vorliegen von legiti-

men Interessen ohne eine explizite Verpflichtung zur Vornahme einer Interessenabwägung eine Datenverwendung per se für rechtmäßig erklärt würde.

Kapitel III – Rechte der betroffenen Personen

Neben offenen Problemen in Art. 17, 19 und 20 ist insbesondere folgender Punkt zu Art. 21 von besonderer Bedeutung, welcher festlegt, unter welchen Voraussetzungen der Unions- bzw. Mitgliedstaatsgesetzgeber die Anwendung bestimmter Rechte und Pflichten aus der Verordnung beschränken können. Im vorliegenden Dokument findet sich ein schwer verständlicher Verweis auf Art. 5 („allgemeine Grundprinzipien"), der auch Ausnahmen von diesen Grundprinzipien ermöglicht. Nach österreichischem Verständnis haben jedoch die allgemeinen Grundprinzipien des Datenschutzes in allen Fällen des Anwendungsbereichs der Verordnung zu gelten, sodass Ausnahmen davon nicht möglich sein können. Die allgemeinen Grundprinzipien umfassen etwa Grundsätze wie „Treu und Glauben", „Rechtmäßigkeit" oder das „Verhältnismäßigkeitsprinzip". Vor dem Hintergrund, dass nach österreichischer Ansicht die allgemeinen Grundprinzipien selbst nicht eingeschränkt werden können, erscheint diese Formulierung nicht vertretbar.

Die Prüfung der Zulässigkeit einer Beschränkung dieser Konkretisierungen knüpft innerhalb der Systematik des Art. 21 im Übrigen selbst an das Erfordernis der Verhältnismäßigkeit an („necessary and proportionate measure"). Es ist daher auch unklar, wie dieser Prüfmaßstab in Art. 21 herangezogen werden soll, wenn das Verhältnismäßigkeitsprinzip (über die Aufnahme des Art. 5 in den Ausnahmekatalog des Art. 21) aus dem Art. 21 herausfällt.

Kapitel IV – Für die Verarbeitung Verantwortlicher („Auftraggeber") und Auftragsverarbeiter („Dienstleister")

Art. 33 regelt das sogenannte „Impact Assessment", welches selbstständig vor Durchführung der Datenverarbeitung durch den Auftraggeber durchzuführen ist, wenn die Datenverarbeitung in ein hohes Risiko münden könnte. Art. 34 sieht als weitere Stufe vor, dass die Datenschutzbehörden vorab zu konsultieren sind, wenn das „Impact Assessment" das potentielle hohe Risiko bestätigt und dieses nicht durch Gegenmaßnahmen ausreichend reduziert werden kann. Die Abgrenzung zwischen Art. 33 und Art. 34 ist nach österreichischer Ansicht jedoch unklar.

Österreich ist der Ansicht, dass es bestimmte, besonders sensible Verarbeitungsvorgänge gibt, die zwingend eine Vorabkonsultation der Aufsichtsbehörde auslösen. Um den Auftraggebern die nach Abschluss des autonom durchgeführten „Impact Assessment“ vorzunehmende Entscheidung zu erleichtern, ob ihre Anwendung die Schwelle der Konsultationspflicht nach Art. 34 erreicht, sollte eine exemplarische Liste mit jedenfalls vorabkonsultationspflichtigen Anwendungen vorgesehen werden. Die Listenerstellung sollte den Aufsichtsbehörden obliegen.

Kapitel V – internationaler Datentransfer

Hinsichtlich Kapitel V hat Österreich bereits beim JI-Rat am 5./6. Juni 2014 zur partiellen allgemeinen Ausrichtung zu diesem Kapitel der Datenschutz-Grundverordnung Bedenken geäußert und in einer Erklärung zum Ratsprotokoll dargelegt. Österreich hatte zuvor auch in einem Grundsatzpapier zu Kapitel V (Dok 10198/14) auf diese Problemstellungen hingewiesen und Anregungen vorgenommen. Zur österreichischen Position zu Kapitel V (Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen) ist im Detail Folgendes auszuführen:

Das im Kapitel V enthaltene Grundmodell für die Drittstaatsübermittlung folgt im Wesentlichen weitgehend der Systematik der derzeitigen Datenschutz-Richtlinie und kann von Österreich mitgetragen werden. Damit wird Rechtssicherheit und Rechtskontinuität gewährleistet. Einzelne Aspekte dieses Kapitels werfen aus österreichischer Sicht jedoch noch Fragestellungen bzw. Probleme auf:

Art. 41 Abs. 1: Adäquanzentscheidungen für „specified sectors” sollten auf für diesen Sektor rechtsverbindlichen Vorgaben basieren (siehe auch Ausführungen in EG 80).

Art. 41 Abs. 2 lit. a: Bei Adäquanzentscheidungen sollten Faktoren wie Regelungen zur nationalen Sicherheit etc. mitberücksichtigt und (wie im EK- und EP-Vorschlag) wieder in den Kriterienkatalog des normativen Verordnungstextes aufgenommen werden.

Dem Grundprinzip des Art. 42, dass ein Datentransfer bei Vorliegen einer rechtsverbindlichen Grundlage mit durchsetzbaren Rechten der betroffenen Personen ohne zusätzliche Genehmigung der Aufsichtsbehörde erfolgen kann, kann Österreich zustimmen. Ob diese Voraussetzungen nach der derzeitigen Textfassung des Art. 42 des Verordnungsentwurfs auch bei Verhaltenskodizes und Zertifizierungen gemäß Abs. 2

lit. d und e leg. cit. zutreffen, erscheint unklar. Hinsichtlich der Anforderungen für Datenübermittlungen im öffentlichen Bereich (auch im Hinblick auf Verwaltungsübereinkommen [„administrative arrangements“] gemäß Art. 42 Abs. 2a lit. d) hat sich Österreich für eine Klarstellung dahingehend eingesetzt, dass nur rechtsverbindliche Instrumentarien (im Lichte der Vorgaben der EU-Grundrechte-Charta für Grundrechtseingriffe möglicherweise sogar nur auf gesetzlicher Ebene [„by law“]) in Frage kommen sollen.

Die in Art. 44 Abs. 1 lit. h enthaltene Ausnahmeregelung für eine Datenübermittlung in einen Drittstaat bei bloßem Vorliegen eines „berechtigten Interesses“ des Auftraggebers, das nicht von einem Interesse oder Grundrecht des Betroffenen überwogen wird, wurde von Österreich stets abgelehnt. Die Entscheidung über eine Datenübermittlung in einen Drittstaat wird mit dieser Regelung nämlich weitgehend in die eigenständige Entscheidungsbefugnis des Auftraggebers übertragen, ohne dass vorab die Datenschutzbehörde regulierend eingreifen kann. Ein (nur) berechtigtes Interesse des Auftraggebers an einem Auslandsdatentransfer kann – auch unter den einschränkenden aber vage gehaltenen Bedingungen dieser Regelung („nicht in großem Maßstab oder häufig“, „geeignete Garantien“) – keine geeignete Rechtsgrundlage für eine Übermittlung sein. Bei der Regelung handelt es sich nach österreichischer Ansicht um eine „generalklauselartige“ Ermächtigung und somit um eine im Gesamtkonzept der Auslandsdatenübermittlung systemwidrige Regelung: Das grundsätzlich strenge Gesamtregime für Auslandsdatenübermittlungen im Hinblick auf die erforderliche Adäquanz der Datenschutzstandards, im Hinblick auf Standardvertragsklauseln, Binding Corporate Rules etc. könnte damit leicht umgangen werden. Auch wenn dieser Bestimmung von der Grundintention nur Ausnahmecharakter zukommen soll, besteht die Gefahr einer künftigen extensiven Auslegung. Im Ergebnis könnte diese Ausnahmebestimmung damit zum Regelfall für Auslandsdatenübermittlungen werden. Im Übrigen wird darauf hingewiesen, dass auch das EP in seiner Position zur Datenschutz-Grundverordnung vom 12. März 2014 die Streichung der lit. h leg. cit. vorgeschlagen hat bzw. dass auch die derzeit geltende DS-RL eine derartige Ausnahmebestimmung nicht kennt. Die im Zuge des Trilogs im Juli 2015 als Kompromiss gehandelte Regelungsvariante, dass zusätzlich zu den bisherigen Kriterien vom Auftraggeber eine verpflichtende Information an die Aufsichtsbehörde und den Betroffenen zu ergehen hat, wurde von Österreich nicht unterstützt (akzeptabel allenfalls: Genehmigung durch die Aufsichtsbehörde).

Darüber hinaus erfolgte bislang noch keine tiefergehende Auseinandersetzung mit dem Textvorschlag des EP zu Art. 43a („Anti-Fisa-Regelung“ – Datenübermittlung durch Unternehmen an Behörden in Drittstaaten) sowie dem korrespondierenden Vorschlag Deutschlands zu Art. 42a (Dok 12884/13), welche nach österreichischer Ansicht wichtige Aspekte behandeln.

Kapitel VI und VII – Zentrale Kontaktstelle (One-Stop-Shop-Prinzip)

Hinsichtlich des Prinzips der zentralen Kontaktstelle konnte Österreich beim JI-Rat am 12./13. März 2015 der partiellen allgemeinen Ausrichtung – trotz punktuell bestehender Bedenken – zustimmen. Folgende Problempunkte wurden im Zusammenhang mit der zentralen Kontaktstelle (im Wesentlichen Kapitel VI und VII der Datenschutz-Grundverordnung) im Vorfeld im Detail diskutiert:

Behandlung „lokaler Fälle“ (Art. 51a Abs. 2a bis 2d und EG 97)

Generell unterliegt die lokale Behörde einer Mitteilungspflicht an die federführende Aufsichtsbehörde (DPA), welche den Fall quasi an sich ziehen kann, wenn sie der Meinung ist, dass es sich nicht um einen lokalen Fall handelt. Dabei hat sie mit Blick auf die Sicherstellung der effektiven Durchsetzbarkeit einer Entscheidung zu berücksichtigen, ob eine Niederlassung im Mitgliedstaat der betroffenen Behörde vorhanden ist. Sollte die federführende Aufsichtsbehörde den Fall an sich ziehen, kommt das One-Stop-Shop-Prozedere (OSS-Prozedere) zur Anwendung (siehe Art. 54a), wobei in diesem Fall die lokale Behörde einen Entscheidungsentwurf erstellen kann, der tunlichst von der federführenden Aufsichtsbehörde zu berücksichtigen ist („trägt diesem Entwurf … weitestgehend Rechnung“). Sollte dies nicht der Fall sein, besteht die allgemeine Möglichkeit des Einspruchs durch die lokale Behörde. Sollte die federführende Aufsichtsbehörde den Fall nicht an sich ziehen, entscheidet die lokale Behörde autonom allenfalls unter Rückgriff auf die gegenseitige Amtshilfe (Art. 55) bzw. auf die gemeinsamen Maßnahmen der Aufsichtsbehörden (Art. 56).

Bis zuletzt stand auch eine weitere – auch von Österreich unterstützte – Variante im Raum: Sollte die federführende Aufsichtsbehörde den Fall an sich ziehen, kommt das allgemeine OSS-Prozedere (Art. 54a) zum Tragen. Sollte die federführende Aufsichtsbehörde dies nicht tun, sollte die lokale Aufsichtsbehörde einen Entscheidungsvorschlag erarbeiten, der letztlich wiederum durch die federführende Aufsichtsbehörde (gemäß Art. 54a Abs. 4a, 4b, 4bb) angenommen werden muss, sofern inhaltliche Einig-

keit besteht. Dieses Verfahren wurde vorgesehen, um letztlich schwer lösbare Fragen der Durchsetzbarkeit der Entscheidungen von (nur) lokalen Behörden in anderen Mitgliedstaaten zu vermeiden. Sollte keine inhaltliche Einigkeit über den Entscheidungsvorschlag der lokalen DPA bestehen, kommt das gesamte OSS-Prozedere des Art. 54a (mit inhaltlicher Einspruchsmöglichkeit der lokalen DPA gegen den Entscheidungsvorschlag der federführenden Aufsichtsbehörde) zum Tragen. Österreich sprach sich bis zuletzt für diese Variante aus, da diese weniger Fragen zur Durchsetzbarkeit der Entscheidungen nationaler Behörden in anderen Mitgliedstaaten aufwirft (etwa in lokalen Fällen, in denen es keine Niederlassung des Auftraggebers im Mitgliedstaat der lokalen Behörde gibt). Bei der nunmehr vorliegenden Lösung hängt die Effizienz des Mechanismus letztlich von der Ausübung des Ermessens der federführenden Aufsichtsbehörde ab, dh. ob sie – etwa bei Fehlen einer Niederlassung am Sitz der lokalen Behörde – den Fall an sich zieht oder nicht.

Frage einer quantitativen Schwelle zur Einbeziehung des Europäischen Datenschutzausschusses (EDPB; Art. 54a Abs. 3)

Seitens einiger Mitgliedstaaten bestand die Befürchtung, dass das EDPB mit einer Fülle von Fällen überhäuft werden könnte. Es wurde daher zunächst eine qualitative Schwelle für die Erhebung eines Einspruchs durch die betroffenen Behörden hinsichtlich der vorgeschlagenen Entscheidung der federführenden Aufsichtsbehörde eingeführt: Es müsse sich um einen „relevanten und begründeten Einspruch“ handeln. Die zusätzliche Einführung eines quantitativen Kriteriums dahingehend, dass eine bestimmte (Mindest-)Anzahl von betroffenen Datenschutzbehörden (etwa eine Schwelle von 1/3 der betroffenen Datenschutzbehörden) erforderlich ist, um Einspruch gegen die Entscheidung der federführenden Aufsichtsbehörde erheben zu können, fand keine Mehrheit. Auch der JDR sprach sich gegen die Aufnahme eines quantitativen Kriteriums aus, da damit die geforderte Bürgernähe nicht sichergestellt werden kann. Österreich hat sich gegen die Einführung eines quantitativen Kriteriums ausgesprochen; jede betroffene Datenschutzbehörde soll die Möglichkeit haben, bei gravierenden Bedenken den Fall zum EDPB zu bringen.

Anfechtung der verbindlichen Entscheidungen des EDPB (Art. 58a Abs. 6 und Abs. 7, Art. 76b)

Art. 263 AEUV sieht ein Rechtsmittel an den EuGH in Form einer Nichtigkeitsklage zur Überwachung der Rechtmäßigkeit von Handlungen der Einrichtungen oder sonstigen

Stellen der Union mit Rechtswirkung gegenüber Dritten vor. Dies wird auch gegenüber Entscheidungen des EDPB zu gelten haben (Art. 263 Abs. 4 AEUV). Ebenso möglich ist ein Vorabentscheidungsverfahren (Auslegung oder Gültigkeitsentscheidung) durch nationale Gerichte nach Art. 267 AEUV.

Das gegenwärtige OSS-System sieht vor, dass nationale DPAs die Entscheidungen des EDPB umzusetzen haben. Die betroffene Person kennt daher den vollen Umfang einer Entscheidung erst dann, wenn nach dem EDPB die Entscheidung der zuständigen nationalen Behörde vorliegt. Daraus entstehen Fragen zum Fristablauf hinsichtlich der Geltendmachung von Rechtsmitteln gegenüber der Entscheidung des EDPB. Art. 263 Abs. 6 AEUV sieht für die Einbringung einer Nichtigkeitsklage eine Frist von zwei Monaten vor. Diese Frist läuft je nach Lage des Falles von der Bekanntgabe der betreffenden Handlung, ihrer Mitteilung an den Kläger oder in Ermangelung dessen von dem Zeitpunkt an, zu dem der Kläger von dieser Handlung Kenntnis erlangt hat. Der Kläger wird jedoch im OSS-Bereich oft die Entscheidung der nationalen Behörde abwarten, sodass es uU zu einem Fristablauf hinsichtlich der Nichtigkeitsklage gegen eine EDPB-Entscheidung kommen kann. Grundsätzlich könnte der Betroffene zwar die Entscheidung der nationalen DPA vor den nationalen Gerichten anfechten, diese sind jedoch im Verfahren an die EDPB-Entscheidung gebunden und können diese auch nicht mehr mittels Vorabentscheidungsverfahren anfechten, da der Betroffene nicht von seinen Möglichkeiten nach Art. 263 AEUV Gebrauch gemacht hat.

Der Großteil der Delegationen – so auch Österreich – präferierte die Lösung, wonach die Frist nach Art. 263 AEUV erst nach (verpflichtender) Veröffentlichung der EDPB-Entscheidung zu laufen beginnt (siehe Art. 58a Abs. 6 und 7 sowie EG 113). Die Veröffentlichung würde auf der EDPB-Website erfolgen (auch ohne Bezug auf Personennamen, wenn dies erforderlich ist). Gleichzeitig müsse ein Mechanismus vorgesehen werden, dass die Veröffentlichung erst nach Vorliegen der nationalen DPA-Entscheidung erfolgt, dafür bedarf es eines Notifzierungssystems.

Von besonderer Bedeutung für Österreich ist, dass in jedem Fall alle EDPB-Entscheidungen sowie die Gruppen-Entscheidungen, welche nicht vor dem EDPB angefochten werden, zu veröffentlichen sind. Dies müsste unabhängig von der hier diskutierten Frage der allfälligen Rechtsmittel im Hinblick auf die notwendige Transparenz der Entscheidungen jedenfalls gelten. Angeregt wurde auch, in Art. 66 (Aufgaben des

EDPB) anzuordnen, dass die Publikation der Entscheidung in allen Amtssprachen zu erfolgen hat und dass die Zugänglichkeit via Web zumindest anhand der Norm und anhand von Schlagwörtern gewährleistet sein sollte.

Sicherstellung des Sekretariats des EDPB (Art. 71)

Das EDPB setzt sich aus den Vorsitzenden der MS-Datenschutzbehörden zusammen. Art. 71 sieht derzeit vor, dass das Sekretariat beim Europäischen Datenschutzbeauftragen (European Data Protection Supervisor – EDPS) angesiedelt sein soll. Weiters ist vorgesehen, dass die Unabhängigkeit des EDPB-Personals sicherzustellen ist und das EDPB-Personal nicht den Weisungen des EDPS unterliegt. Das EDPB wird hinsichtlich der verbindlichen Entscheidungsbefugnis mit Rechtspersönlichkeit ausgestattet.

Seitens Österreichs bestand kein Einwand gegen ein gemeinsames Sekretariat von EDPS und EDPB unter den oben genannten Prämissen. Von Österreich wurde zusätzlich angeregt, in der Verordnung ausdrücklich klarzustellen, dass der EDPS ausreichend personelle und sachliche Ressourcen bereitstellen muss, damit die Arbeit des EDBP und Weisungen des EDPB-Vorsitzes ausgeführt werden können.

Art. 4 Abs. 13 – „Hauptniederlassung“ und damit im Zusammenhang das OSS-Register (Art. 51c)

In der vorliegenden Fassung der Definition stellt sich insbesondere die Frage, wer verbindlich feststellt, wo die Entscheidung des Unternehmens getroffen wird. Dabei handelt es sich um eine Festlegung, die letztlich im Ermessen der Unternehmensorganisation liegt und die – in Ermangelung entsprechender Vorgaben in der Grundverordnung – durch das Unternehmen selbst im Anlassfall gegebenenfalls auch kurzfristig geändert werden könnte. Von außen ist die Überprüfung der Plausibilität einer solchen Unternehmensentscheidung schwierig bis unmöglich. Im Sinne der Transparenz, der Verfahrensökonomie und der Rechtssicherheit erscheint eine verpflichtende Notifikation der Hauptniederlassung an die federführende Aufsichtsbehörde mit anschließender Veröffentlichung in einem Register nicht nur zweckmäßig sondern vielmehr geboten. Damit können auch willkürlich durch Unternehmen veranlasste Wechsel der Zuständigkeiten verhindert werden. Dies steht daher in einem engen Zusammenhang mit den – mittlerweile im vorliegenden Text gestrichenen – Bestimmungen nach Art. 51b (Identification of the supervisory authority competent for the main establishment) und Art. 51c (One-stop-shop register). Österreich hatte sich für die Beibehaltung der

Substanz dieser Bestimmungen ausgesprochen.

Art. 4 Abs. 19b – „grenzüberschreitende Verarbeitung"

Der Fall, dass eine Niederlassung von mehreren Niederlassungen eines Auftraggebers grenzüberschreitend tätig wird (bspw. Kundenbetreuung in mehreren MS), muss nach österreichischer Ansicht unter das OSS-Prozedere fallen. Dieser Fall wäre von der jetzigen Definition im Art. 4 Abs. 19b wohl nicht erfasst und würde daher aus dem OSS fallen. Nach der jetzigen Definition in lit. a leg. cit. müssten wohl immer mehrere Niederlassungen tätig werden, um eine grenzüberschreitende Datenverarbeitung darzustellen und damit das OSS-Prozedere iS von Art. 51a auszulösen. Daher sollte die Nennung von „Niederlassung" in Art. 4 Abs. 19b lit. a in der Einzahl und Mehrzahl erfolgen.

Art. 4 Abs. 19c – „relevanter und begründeter Einspruch"

Österreich hat sich dafür ausgesprochen, den zweiten Satz in die Erwägungsgründe zu verschieben, um die Anforderungen für die lokale Datenschutzbehörde nicht zu hoch anzusetzen.

Art. 51 Abs. 2 – Ausnahme von OSS (siehe FN 22)

Es ist aus österreichischer Sicht nicht nachvollziehbar, warum sämtliche private Unternehmen, welche einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 lit. c zu einer Datenverwendung unterliegen, aus dem OSS-System herausfallen sollen. Dies könnte zur Konsequenz haben, dass in einem Unternehmen vereinzelte Anwendungen wie etwa Rechnungslegungsverpflichtungen dem OSS nicht unterliegen, andere Datenverwendungen hingegen schon.

Art. 58a – Beschlüsse des Europäischen Datenschutzausschusses (EDPB)

Nach österreichischer Auffassung sollte im Entscheidungsfindungsprozess von Beginn an auf eine einfache Mehrheit abgestellt werden. Das vorgesehene abgestufte Modell, wonach sich durch bloßen Zeitablauf das Erfordernis der 2/3-Mehrheit in das einer einfachen Mehrheit umwandelt, führt nach österreichischer Ansicht nur zur Verlängerung des Verfahrens und bringt keinen Mehrwert.

3. Auswirkungen auf die österreichische Gesetzeslage

Die vorgeschlagene Datenschutz-Grundverordnung wäre bedingt durch die gewählte Rechtsaktform der Verordnung gemäß Art. 288 Abs. 2 AEUV in Österreich unmittelbar gültig und anwendbar und bedürfte daher keiner nationalen Umsetzung.

Da der Verordnungsentwurf einige Bereiche vorsieht, in denen die Mitgliedstaaten nationale Vorschriften zu erlassen haben, müssten diese – ebenso wie etwa organisatorische Regelungen oder Datenschutzregelungen außerhalb des Anwendungsbereichs des Unionsrechts – in einem entsprechenden nationalen Ausführungsgesetz geregelt werden bzw. müssten Ausführungsbestimmungen in bestehende Materiengesetze aufgenommen werden. Es bedürfte daher einer grundlegenden Neugestaltung des DSG 2000.

4. Finanzielle Auswirkungen

Die Vereinheitlichung des allgemeinen Datenschutzes in der EU sowie der Entfall der Meldepflicht von Datenanwendungen würden allgemein zu noch nicht bezifferbaren Einsparungseffekten bei Unternehmen und öffentlichen Stellen führen. Die EK geht davon aus, dass durch eine einheitliche Regelung das Vertrauen der Konsumenten in den elektronischen Handel steigt und dieser dadurch – mit positivem Effekt für die Wirtschaft – wächst.

Dem stünden Kosten für die allgemeine Dokumentationspflicht der Auftraggeber sowie für die Datenschutz-Folgenabschätzungen gegenüber. Die Verpflichtung zur Einrichtung und ausreichenden Ausstattung der unabhängigen Aufsichtsbehörde würde sich nur im Rahmen neu übertragener Aufgaben finanziell auswirken, zumal eine derartige Aufsichtsbehörde in Form der Datenschutzbehörde (DSB) schon aufgrund der DS-RL verpflichtend einzurichten war und auch eingerichtet wurde.

5. Subsidiaritätsprüfung

Die EK hat die Subsidiarität und die Verhältnismäßigkeit geprüft. Darüber hinaus ergibt sich Folgendes:

Der Verordnungsvorschlag gründet sich insbesondere auf Art. 16 Abs. 2 AEUV, der die Union zur Regelung des Datenschutzes und Datenverkehrs in den Mitgliedstaaten ermächtigt, soweit es Tätigkeiten betrifft, die in den Anwendungsbereich des Unionsrechts fallen. Ausgenommen hievon sind Tätigkeiten im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik.

Das Recht auf Schutz personenbezogener Daten, das in Art. 8 der EU-Grundrechte-Charta verankert ist, verlangt ein unionsweit einheitliches Datenschutzniveau. Ohne harmonisierte unionsrechtliche Vorschriften zum Datenschutz bestünde die Gefahr, dass der Datenschutz in den Mitgliedstaaten nicht in gleichem Maße gewährleistet ist, was – insbesondere im Hinblick auf die zunehmende grenzüberschreitende Datenverwendung und Vernetzung – aus datenschutzrechtlicher und datenschutzpolitischer Sicht nicht tragbar erscheint und aus Binnenmarktsicht den grenzüberschreitenden Verkehr personenbezogener Daten zwischen Mitgliedstaaten mit unterschiedlichen Datenschutzanforderungen behindern würde.

Der Transfer personenbezogener Daten sowohl in andere Mitgliedstaaten als auch in Drittstaaten nimmt rasant zu. Die praktischen Schwierigkeiten bei der Durchsetzung der Datenschutzvorschriften und die hierzu notwendige Zusammenarbeit zwischen den Mitgliedstaaten und ihren Behörden erfordern ein Regelwerk auf EU-Ebene, das die einheitliche Anwendung des Unionsrechts gewährleistet. Die EU ist auch die geeignete Ebene, um sicherzustellen, dass alle Betroffenen bei der Übermittlung personenbezogener Daten in Drittländer effektiv in gleichem Maße geschützt sind.

Die Mitgliedstaaten können die derzeitigen Probleme – vor allem die trotz Vorhandensein der DS-RL durch die Uneinheitlichkeit der nationalen Umsetzungsvorschriften bedingten Probleme – nicht allein überwinden. Es besteht daher ein besonderer Bedarf an einer harmonisierten, kohärenten Regelung, die einen reibungslosen Transfer personenbezogener Daten innerhalb der EU ermöglicht und gleichzeitig unionsweit allen Betroffenen einen wirksamen Datenschutz garantiert. Dies scheint effektiv letztlich nur in Form einer Verordnung erfüllbar.

Wegen Art und Umfang der dargelegten Probleme, die nicht auf einen Mitgliedstaat oder mehrere Mitgliedstaaten beschränkt sind, werden die vorgeschlagenen Legislativ-

maßnahmen der EU daher auch unter dem Blickwinkel des Subsidiaritäts- und Verhältnismäßigkeitsprinzips als erforderlich erachtet.