Rat der
Europäischen Union

Brüssel, den 8. April 2016
(OR. en)

5419/1/16
REV 1 ADD 1

Interinstitutionelles Dossier:
2012/0011 (COD)

DATAPROTECT 2
JAI 38
MI 25
DIGIT 21
DAPIX 9
FREMP 4
CODEC 52
PARLNAT 83

ENTWURF DER BEGRÜNDUNG DES RATES

Betr.:	Standpunkt des Rates in erster Lesung im Hinblick auf den Erlass einer VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) – Entwurf der Begründung des Rates - Annahme durch den Rat am 8. April 2016

I. EINLEITUNG

Die Kommission hat am 25. Januar 2012 eine umfassende Datenschutzreform vorgeschlagen und hierzu Folgendes vorgelegt:

– den vorgenannten Vorschlag für eine Datenschutz-Grundverordnung, welche die Datenschutzrichtlinie von 1995 (ehemalige erste Säule) ersetzen soll, sowie

– einen Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, welche den Datenschutz-Rahmenbeschluss von 2008 (ehemalige dritte Säule) ersetzen soll.

Das Europäische Parlament hat seinen Standpunkt in erster Lesung zu der vorgeschlagenen Datenschutz-Grundverordnung am 12. März 2014 festgelegt (Dok. 7427/14).

Der Rat hat am 15. Juni 2015 eine allgemeine Ausrichtung festgelegt und damit dem Vorsitz ein Verhandlungsmandat zur Aufnahme von Trilogen mit dem Europäischen Parlament erteilt (Dok. 9565/15).

Das Europäische Parlament und der Rat haben auf der Ebene des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres bzw. des Ausschusses der Ständigen Vertreter am 17. bzw. 18. Dezember 2015 die Einigung über den aus den Trilog-Verhandlungen hervorgegangenen Kompromisstext bestätigt.

Der Rat hat auf seiner Tagung vom 12. Februar 2016 eine politische Einigung über den Entwurf der Verordnung erzielt (Dok. 5455/15). Der Rat hat am 8. April 2016 seinen Standpunkt in erster Lesung festgelegt, der vollständig dem Kompromisstext der Verordnung entspricht, auf den sich der Rat und das Europäische Parlament im Rahmen der informellen Verhandlungen geeinigt hatten.

Der Wirtschafts- und Sozialausschuss hat 2012 eine Stellungnahme zu der Verordnung abgegeben (ABl. C 229 vom 31.7.2012, S. 90).

Der Wirtschafts- und Sozialausschuss hat eine Stellungnahme zu der Verordnung abgegeben (ABl. C 391 vom 18.12.2012, S. 127).

Der Europäische Datenschutzbeauftragte wurde konsultiert und hat 2012 eine erste Stellungnahme (ABl. C 192 vom 30.6.2012, S. 7) und 2015 eine zweite Stellungnahme (ABl. C 301 vom 12.9.2015, S. 1) abgegeben.

Die Agentur für Grundrechte hat am 1. Oktober 2012 eine Stellungnahme vorgelegt.

II. ZIEL

Durch die Datenschutz-Grundverordnung werden die Datenschutzvorschriften in der Europäischen Union harmonisiert. Ziel der Verordnung ist es, die Datenschutzrechte natürlicher Personen zu stärken, den freien Verkehr personenbezogener Daten im Binnenmarkt zu erleichtern und den Verwaltungsaufwand zu verringern.

III. ANALYSE DES STANDPUNKTS DES RATES IN ERSTER LESUNG

A. Allgemeine Bemerkungen

Angesichts des vom Europäischen Rat angestrebten Ziels, bis Ende 2015 eine Einigung über die Datenschutzreform zu erreichen, haben das Europäische Parlament und der Rat informelle Verhandlungen geführt, um ihre Standpunkte einander anzunähern. Der Wortlaut des Standpunkts des Rates in erster Lesung zur Datenschutz-Grundverordnung spiegelt den zwischen den beiden Gesetzgebern erzielten Kompromiss, der mit Unterstützung der Europäischen Kommission zustande gekommen ist, voll und ganz wider.

Der Rat hält in seinem Standpunkt in erster Lesung an den Zielen der Richtlinie 95/46/EG – d.h. Schutz der Datenschutzrechte und freier Datenverkehr – fest. Parallel dazu strebt er angesichts der stetig wachsenden Menge personenbezogener Daten, die infolge des technologischen Wandels und der Globalisierung verarbeitet werden, nach einer Anpassung der derzeit geltenden Datenschutzvorschriften. Im Hinblick auf eine zukunftssichere Gestaltung der Verordnung sind die Datenschutzvorschriften des in erster Lesung festgelegten Standpunkts des Rates in technologischer Hinsicht neutral.

Damit unionsweit ein gleichmäßiges Datenschutzniveau für den Einzelnen gewährleistet ist und Divergenzen, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, vorgebeugt wird, sieht der Standpunkt des Rates in erster Lesung größtenteils ein einheitliches, unmittelbar in der gesamten Union geltendes Regelwerk vor. Durch diese Harmonisierung wird die Fragmentierung überwunden, die durch die unterschiedlichen Gesetze der Mitgliedstaaten zur Umsetzung der Richtlinie 95/46 entstanden war. Trotzdem bietet der Standpunkt des Rates in erster Lesung den Mitgliedstaaten die Möglichkeit, in ihrem nationalen Recht näher auszuführen, wie die in der Verordnung festgelegten Datenschutzvorschriften anzuwenden sind, damit den Anforderungen für besondere Verarbeitungssituationen – auch im öffentlichen Sektor – Rechnung getragen wird.

Der Schutz personenbezogener Daten ist ein Grundrecht, das in Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union verankert ist. Zudem ist in Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union festgelegt, dass jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat, ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts, und dass sowohl für diesen Zweck als auch für den des freien Verkehrs personenbezogener Daten Vorschriften erlassen werden sollten. Auf dieser Grundlage sind im Standpunkt des Rates in erster Lesung die Grundsätze und Vorschriften für den Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten niedergelegt.

Damit die Ziele der Verordnung erreicht werden, wird im Standpunkt des Rates in erster Lesung die Rechenschaftspflicht der Verantwortlichen (zuständig für die Festlegung der Zwecke und Mittel der Verarbeitung personenbezogener Daten) und der Auftragsverarbeiter (zuständig für die Verarbeitung personenbezogener Daten im Namen des Verantwortlichen) verstärkt, um eine wirkliche Datenschutzkultur zu fördern. Vor diesem Hintergrund wird für die gesamte Verordnung ein risikobasierter Ansatz eingeführt, der es ermöglicht, die Pflichten des Verantwortlichen und des Auftragsverarbeiters entsprechend dem Risiko der von ihnen vorgenommenen Datenverarbeitung anzupassen. Ferner tragen Verhaltensregeln und Zertifizierungsverfahren dazu bei, dass die Datenschutzvorschriften eingehalten werden. Bei diesem Ansatz werden übermäßig präskriptive Vorschriften vermieden und der Verwaltungsaufwand verringert, ohne dass dies hinsichtlich der Einhaltung der Vorschriften zu Abstrichen führt. Der abschreckende Charakter potenzieller Sanktionen, die verhängt werden können, schafft für die Verantwortlichen einen Anreiz, die Verordnung einzuhalten.

Die im Standpunkt des Rates in erster Lesung festgelegten neuen Datenschutzvorschriften sehen auch stärkere und durchsetzbare Rechte für die Bürger vor. Dies ermöglicht dem Einzelnen eine bessere Kontrolle über seine personenbezogenen Daten, was dazu führt, dass den Online-Diensten grenzübergreifend mehr Vertrauen entgegengebracht wird und infolgedessen dem digitalen Binnenmarkt Impulse verliehen werden. Kinder verdienen besonderen Schutz, da sie sich sowohl der Risiken, die mit der Verarbeitung personenbezogener Daten verbunden sind, als auch ihrer Rechte weniger bewusst sein dürften.

Ferner wird den Aufsichtsbehörden im Standpunkt des Rates in erster Lesung mehr Unabhängigkeit eingeräumt, während gleichzeitig ihre Aufgaben und Befugnisse harmonisiert werden. Die Vorschriften über die Zusammenarbeit zwischen den Aufsichtsbehörden und gegebenenfalls mit der Kommission in grenzübergreifenden Fällen – d.h. das Kohärenzverfahren – wird zu einer einheitlichen Anwendung der Verordnung in der gesamten Union beitragen. Dies wird die Rechtssicherheit erhöhen und den Verwaltungsaufwand verringern. Außerdem wird mit dem Prinzip der zentralen Anlaufstelle dafür gesorgt, dass es einen einzigen Ansprechpartner der Verantwortlichen oder der Auftragsverarbeiter für Fragen der von ihnen durchgeführten grenzüberschreitenden Verarbeitung gibt, einschließlich verbindlicher Beschlüsse des neu geschaffenen Europäischen Datenschutzausschusses in Streitfällen. Aufgrund dieses Verfahrens wird die Anwendung der Verordnung einheitlicher sein. Zudem wird es mehr Rechtssicherheit bieten und den Verwaltungsaufwand verringern.

Schließlich wird im Standpunkt des Rates in erster Lesung ein umfassender Rahmen für die Übermittlung personenbezogener Daten aus der Europäischen Union an Empfänger in Drittländern oder internationale Organisationen festgelegt, der im Vergleich zur Richtlinie 95/46/EG neue Instrumente vorsieht.

B. Kernpunkte

Der Rat und das Europäische Parlament haben mit Unterstützung der Kommission im Wege informeller Verhandlungen ihre Standpunkte, die in der allgemeinen Ausrichtung des Rates bzw. im Standpunkt des Parlaments in erster Lesung niedergelegt sind, einander angenähert. Der Standpunkt des Rates in erster Lesung zur Datenschutz-Grundverordnung spiegelt die erzielten Kompromisse voll und ganz wider. Die Kernpunkte des Standpunkts des Rates in erster Lesung sind nachstehend dargelegt.

1. Anwendungsbereich

1.1. Sachlicher Anwendungsbereich der Verordnung und Abgrenzung gegenüber der Richtlinie zum Datenschutz bei der Strafverfolgung

Gemäß dem Standpunkt des Rates in erster Lesung gilt die Datenschutz-Grundverordnung für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die Teil einer strukturierten Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, sind oder sein sollen. Der sachliche Anwendungsbereich der Datenschutz-Grundverordnung und der Anwendungsbereich der Richtlinie zum Datenschutz bei der Strafverfolgung schließen sich gegenseitig aus. Es ist festgelegt, dass die Verordnung keine Anwendung auf die Verarbeitung von Daten findet, die durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung vorgenommen wird, was den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit einschließt. Diese Abgrenzung ermöglicht es den Strafverfolgungsbehörden, insbesondere der Polizei, grundsätzlich die Datenschutzregelung der Richtlinie anzuwenden und dabei ein gleichmäßig hohes Maß an Schutz für die personenbezogenen Daten strafrechtlich verfolgter Personen zu gewährleisten.

1.2. Organe und Einrichtungen der EU

Mit dem Ziel, einen einheitlichen und kohärenten Schutz der betroffenen Personen bei der Verarbeitung ihrer personenbezogener Daten zu gewährleisten, wird in dem Standpunkt des Rates in erster Lesung darauf hingewiesen, dass im Anschluss an den Erlass der Datenschutz-Grundverordnung die erforderlichen Anpassungen der Verordnung (EG) Nr. 45/2001, die für die Organe, Einrichtungen, Ämter und Agenturen der EU gilt, vorgenommen werden sollten, damit sie gleichzeitig mit der Datenschutz-Grundverordnung angewandt werden kann.

1.3. Ausnahmeregelung für Privathaushalte

Damit keine Vorschriften festgelegt werden, die unnötigen Aufwand für den Einzelnen mit sich bringen, sieht der Standpunkt des Rates in erster Lesung vor, dass die Verordnung nicht für die Verarbeitung von personenbezogenen Daten gilt, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird.

1.4. Räumlicher Anwendungsbereich

Der Standpunkt des Rates in erster Lesung schafft hinsichtlich des räumlichen Anwendungsbereichs gleiche Ausgangsbedingungen für die Verantwortlichen und die Auftragsverarbeiter, da sie für alle Verantwortlichen und alle Auftragsverarbeiter gilt, unabhängig davon, ob sie in der Union niedergelassen sind oder nicht.

Erstens ist in der Verordnung festgelegt, dass die Datenschutzvorschriften auf die Verarbeitung personenbezogener Daten Anwendung finden, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet oder nicht. Zweitens: Damit einer Person der Schutz ihrer Daten nicht vorenthalten wird, gilt die Verordnung auch dann für die Verarbeitung personenbezogener Daten von in der Union aufhältigen betroffenen Personen, wenn ein Verantwortlicher oder ein Auftragsverarbeiter zwar nicht in der Union niedergelassen ist, aber die Verarbeitung im Zusammenhang damit steht, diesen Personen Waren oder Dienstleistungen in der Union anzubieten sowie ihr Verhalten zu beobachten, soweit ihr Verhalten in der Europäischen Union erfolgt. Außerdem wird durch eine derartige Festlegung des Anwendungsbereichs mehr Rechtssicherheit für die Verantwortlichen und die betroffenen Personen – d.h. für die Einzelnen, deren personenbezogene Daten verarbeitet werden – geschaffen.

Der Standpunkt des Rates in erster Lesung stellt zudem sicher, dass betroffene Personen und Aufsichtsbehörden eine Anlaufstelle in der EU haben, wenn der Verantwortliche oder der Auftragsverarbeiter zwar nicht in der Union niedergelassen ist, sich jedoch der Anwendungsbereich der Verordnung auf ihn erstreckt: In diesem Fall muss er schriftlich einen Vertreter in der Union benennen. Um unnötigen Verwaltungsaufwand zu vermeiden, gilt diese Verpflichtung weder für eine Verarbeitung, die voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt, noch für die Verarbeitung durch eine Behörde oder eine öffentliche Stelle des betreffenden Drittlands.

2. Grundsätze für die Verarbeitung personenbezogener Daten

Die Grundsätze des Datenschutzes gelten für alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, einschließlich der Informationen, die ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (Pseudonymisierung). Verglichen mit der Richtlinie 95/46/EG sorgt die Verordnung für ein hohes Maß an Kontinuität, was die Grundsätze für die Verarbeitung personenbezogener Daten anbelangt. Gleichzeitig wurde der Grundsatz der "Datenminimierung" angepasst, um die digitale Realität zu berücksichtigen und ein ausgewogenes Verhältnis zwischen dem Schutz der personenbezogenen Daten einerseits und den Möglichkeiten, die den Verantwortlichen bei der Datenverarbeitung zur Verfügung stehen, andererseits herzustellen.

3. Rechtmäßigkeit der Verarbeitung

3.1. Bedingungen für die Rechtmäßigkeit

Damit für Rechtssicherheit gesorgt ist, baut der Standpunkt des Rates in erster Lesung auf der Richtlinie 95/46/EG auf und sieht demzufolge vor, dass die Verarbeitung personenbezogener Daten nur dann rechtmäßig ist, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

– Einwilligung der betroffenen Person für einen oder mehrere bestimmte Zwecke;

– Vorliegen eines Vertrags;

– Vorliegen einer rechtlichen Verpflichtung;

– Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person;

– Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

– Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten.

Zwei dieser Bedingungen verdienen eine nähere Betrachtung, nämlich die Einwilligung und die berechtigten Interessen des Verantwortlichen oder eines Dritten.

3.1.1. Einwilligung

Um die Verarbeitung ihrer personenbezogenen Daten zu ermöglichen, kann eine betroffene Person ihre Einwilligung zu der Verarbeitung in Form einer eindeutigen bestätigenden Handlung erteilen, mit der sie freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich bekundet, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Diese Einwilligung bezieht sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge. Wenn die Verarbeitung mehreren Zwecken dient, muss für sämtliche Verarbeitungszwecke eine Einwilligung erteilt werden. Außerdem muss der Verantwortliche nachweisen können, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang erteilt hat. Stillschweigendes Einverständnis, standardmäßig angekreuzte Kästchen oder Untätigkeit der betroffenen Person stellen daher keine Einwilligung dar. Der Begriff "Einwilligung" ist so definiert, dass der Besitzstand, der sich hinsichtlich der Verwendung dieses Begriffs auf der Grundlage der Richtlinie 95/46/EG herausgebildet hat, gewahrt bleibt und gleichzeitig zu einer einheitlichen Auslegung und Anwendung dieses Begriffs in der gesamten Europäischen Union beigetragen wird.

Außerdem ist zum Schutz der Datenschutzrechte der betroffenen Person festgelegt, dass dann, wenn die betroffene Person ihre Einwilligung in Form einer schriftlichen Erklärung erteilt hat, die noch andere Sachverhalte betrifft, jeder Teil dieser Erklärung, der einen Verstoß gegen die Verordnung darstellt, nicht verbindlich ist. Überdies muss bei der Beurteilung der Frage, ob die Einwilligung freiwillig erteilt wurde, in größtmöglichem Umfang berücksichtigt werden, ob unter anderem die Erfüllung eines Vertrags von der Einwilligung zu einer Verarbeitung abhängig gemacht wird, die für die Erfüllung des Vertrags nicht erforderlich ist.

Damit schließlich Ausnahmen vom allgemeinen Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten zugelassen werden können, ist im Standpunkt des Rates in erster Lesung eine höhere Schwelle als für die Verarbeitung anderer Kategorien personenbezogener Daten vorgesehen, da die betroffene Person in die Verarbeitung solcher sensiblen personenbezogenen Daten ausdrücklich einwilligen muss.

Was Kinder anbelangt, so sieht der Standpunkt des Rates in erster Lesung eine besondere Schutzregelung für die Einwilligung von Kindern in Bezug auf das Angebot von Diensten der Informationsgesellschaft vor. Die Verarbeitung der personenbezogenen Daten eines Kindes bis zum vollendeten sechzehnten Lebensjahr ist rechtmäßig, wenn unter Berücksichtigung der verfügbaren Technik angemessen nachgeprüft werden kann, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird. Die Mitgliedstaaten, die eine niedrigere Altersgrenze für angemessener halten, dürfen eine niedrigere Altersgrenze, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf, festlegen.

3.1.2. Berechtigtes Interesse des Verantwortlichen

Die Verarbeitung personenbezogener Daten kann rechtmäßig sein, wenn sie zur Wahrung der berechtigten Interessen eines Verantwortlichen oder eines Dritten erforderlich ist. Diese berechtigten Interessen stellen jedoch keine ausreichende Begründung für die Rechtmäßigkeit der Verarbeitung dar, wenn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Das Bestehen eines berechtigten Interesses erfordert eine Abwägung, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden. Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, gilt dies nicht für die Verarbeitung personenbezogener Daten durch Behörden, die diese in Erfüllung ihrer Aufgaben vornehmen.

3.2. Spezifische Vorschriften der Mitgliedstaaten zur Anpassung der Anwendung der Verordnung

Der Standpunkt des Rates in erster Lesung gestattet es den Mitgliedstaaten, spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der Verordnung beizubehalten oder einzuführen, wenn die personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung verarbeitet werden oder dies für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Ferner sind für spezifische Verarbeitungsvorgänge Ausnahmen, spezifische Anforderungen und andere Maßnahmen vorgesehen, mit denen die Mitgliedstaaten das Recht auf den Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung und Information, dem Zugang der Öffentlichkeit zu amtlichen Dokumenten, der Verarbeitung nationaler Kennziffern, der Verarbeitung im Beschäftigungskontext und der Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Zwecken oder zu statistischen Zwecken in Einklang bringen.

3.3. Weiterverarbeitung

Der Standpunkt des Rates in erster Lesung sieht vor, dass die Verarbeitung für einen anderen Zweck als den, für den die personenbezogenen Daten ursprünglich erhoben wurden, nur dann rechtmäßig ist, wenn diese Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. Hat die betroffene Person jedoch ihre Einwilligung erteilt oder beruht die Verarbeitung auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses darstellt, so darf der Verantwortliche die personenbezogenen Daten ungeachtet der Vereinbarkeit der Zwecke weiterverarbeiten. Die Rechte der betroffenen Person im Falle der Weiterverarbeitung wurden gestärkt, und zwar insbesondere hinsichtlich des Rechts auf Unterrichtung und das Recht, Widerspruch gegen eine solche Weiterverarbeitung einzulegen, wenn diese nicht für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist.

Um sich zu vergewissern, dass ein Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, muss der Verantwortliche unter anderem prüfen, ob ein Zusammenhang zwischen den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung besteht, in welchem Kontext die personenbezogenen Daten erhoben wurden, insbesondere die vernünftigen Erwartungen der betroffenen Person, die auf ihrem Verhältnis zu dem Verantwortlichen beruhen, in Bezug auf die weitere Verwendung dieser Daten, um welche Art von personenbezogenen Daten es sich handelt, welche Folgen die beabsichtigte Weiterverarbeitung für die betroffene Person hat und ob sowohl beim ursprünglichen als auch beim beabsichtigten Weiterverarbeitungsvorgang geeignete Garantien bestehen.

3.4. Verarbeitung besonderer Kategorien von personenbezogenen Daten

Personenbezogene Daten, die ihrem Wesen nach besonders sensibel sind, bedürfen eines besonderen Schutzes, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen auftreten können. Daher behält der Standpunkt des Rates in erster Lesung grundsätzlich den Ansatz der Richtlinie 95/46/EG bei, indem er die Verarbeitung besonderer Kategorien personenbezogener Daten verbietet.

Abweichend von dieser allgemeinen Regel ist die Verarbeitung sensibler Daten unter bestimmten, erschöpfend aufgelisteten Umständen zulässig, beispielsweise wenn die betroffene Person ausdrücklich eingewilligt hat oder wenn die Verarbeitung aus Gründen eines wichtigen öffentlichen Interesses oder für andere Zwecke – unter anderem im Gesundheitsbereich – erforderlich ist.

Schließlich sieht der Standpunkt des Rates in erster Lesung vor, dass die Mitgliedstaaten zusätzliche Bedingungen, einschließlich Beschränkungen, einführen können, soweit die Verarbeitung von genetischen, biometrischen oder gesundheitlichen Daten betroffen ist. Diese Bedingungen dürfen jedoch den freien Datenverkehr innerhalb der Union nicht behindern.

4. Stärkung der Stellung der betroffenen Personen

4.1. Einleitung

Der Standpunkt des Rates in erster Lesung stärkt die Stellung der betroffenen Personen, indem er ihnen verstärkte Datenschutzrechte verleiht und den Verantwortlichen Pflichten auferlegt. Die Rechte der betroffenen Person umfassen folgende Rechte: Recht auf Unterrichtung; Recht auf Zugang zu personenbezogenen Daten; Recht auf Berichtigung; Recht auf Löschung personenbezogener Daten, einschließlich des "Rechts auf Vergessenwerden"; Recht auf Einschränkung der Verarbeitung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; ferner das Recht, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruht. Die Rechte, an denen gegenüber der Richtlinie 95/46/EG bedeutende Änderungen vorgenommen wurden, werden im Folgenden weiter ausgeführt.

Die Verantwortlichen sind verpflichtet, der betroffenen Person im Einklang mit dem Grundsatz der Transparenz die Ausübung ihrer Rechte zu erleichtern, indem sie insbesondere Informationen über die von ihnen durchgeführte Verarbeitung personenbezogener Daten bereitstellen.

Kann der Verantwortliche jedoch anhand der von ihm verarbeiteten personenbezogenen Daten eine betroffene Person nicht identifizieren, so ist er nicht verpflichtet, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu identifizieren.

Unbeschadet dieser Rechte der betroffenen Personen und dieser Verpflichtungen der Verantwortlichen behält der Standpunkt des Rates in erster Lesung den Ansatz der Richtlinie 95/46/EG bei, wonach Beschränkungen der allgemeinen Grundsätze und der persönlichen Rechte zulässig sind, wenn sie auf dem Recht der Union oder der Mitgliedstaaten beruhen. Diese Beschränkungen müssen den Wesensgehalt der Grundrechte und -freiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz bestimmter öffentlicher Interessen darstellen.

4.2. Transparenz

Entsprechend dem Grundsatz der Transparenz müssen die Verantwortlichen Informationen und Mitteilungen, die die Verarbeitung personenbezogener Daten betreffen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermitteln; dies gilt insbesondere für Informationen, die sich an Kinder richten. Die Übermittlung der Informationen muss schriftlich oder in anderer Form, gegebenenfalls auch elektronisch, erfolgen.

Der Standpunkt des Rates in erster Lesung legt ferner Fristen für die Bearbeitung von Anträgen auf Information sowie für Mitteilungen oder andere Maßnahmen des Verantwortlichen fest, die grundsätzlich unentgeltlich zu erfolgen haben. Bei offenkundig unbegründeten oder – insbesondere im Fall ihrer Häufung – unverhältnismäßigen Anträgen einer betroffenen Person kann der Verantwortliche jedoch ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder er kann sich weigern, aufgrund des Antrags tätig zu werden. In diesen Fällen obliegt es dem Verantwortlichen, den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

4.3. Von dem Verantwortlichen bereitzustellende Informationen und Mitteilungen

Damit einerseits die betroffenen Personen ausreichend über die Verarbeitung ihrer personenbezogenen Daten informiert werden, andererseits aber den Verantwortlichen keine übermäßigen Pflichten auferlegt werden, sieht der Standpunkt des Rates in erster Lesung ein Verfahren in zwei Schritten vor, das sicherstellen soll, dass die betroffenen Personen angemessen unterrichtet werden, und zwar sowohl in den Fällen, in denen die personenbezogenen Daten bei der betroffenen Person erhoben werden, als auch in den Fällen, in denen die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden. In einem ersten Schritt muss der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung der personenbezogenen Daten die in der Verordnung aufgeführten Informationen bereitstellen. In einem zweiten Schritt muss er die in der Verordnung aufgeführten zusätzlichen Informationen bereitstellen, die notwendig sind, um eine faire und effiziente Verarbeitung zu gewährleisten. Ferner müssen die Verantwortlichen die betroffenen Personen vorab informieren, wenn sie beabsichtigen, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den diese ursprünglich erhoben wurden.

Der Verantwortliche ist nicht verpflichtet, die im ersten oder im zweiten Schritt zu erteilenden Informationen bereitzustellen, wenn die betroffene Person bereits über diese Informationen verfügt. Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so muss der Verantwortliche die betroffene Person nicht unterrichten, wenn die Speicherung oder Weitergabe der personenbezogenen Daten an Dritte ausdrücklich durch Rechtsvorschriften geregelt ist oder wenn sich die Unterrichtung der betroffenen Person als unmöglich erweist oder mit unverhältnismäßig hohem Aufwand verbunden wäre.

Schließlich sind die Verantwortlichen verpflichtet, allen Empfängern, an die die personenbezogenen Daten weitergegeben wurden, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Ferner muss der Verantwortliche die betroffene Person über diese Empfänger unterrichten, wenn die betroffene Person dies verlangt.

4.4. Bildsymbole

Die Grundsätze einer transparenten Verarbeitung machen es erforderlich, dass die betroffene Person über die Existenz der Verarbeitung und ihre Zwecke unterrichtet wird. Daher ist im Standpunkt des Rates in erster Lesung festgelegt, dass der betroffenen Person Informationen in Kombination mit standardisierten Bildsymbolen bereitgestellt werden können. Die Verantwortlichen können auf freiwilliger Basis entscheiden, ob die Verwendung dieser standardisierten Bildsymbole für die von ihnen durchgeführte Verarbeitung personenbezogener Daten sinnvoll wäre. Die Bildsymbole sollten in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung vermitteln. Sie müssen gleichzeitig mit den Informationen bereitgestellt werden. Werden die Bildsymbole in elektronischer Form dargestellt, so müssen sie maschinenlesbar sein. Um zu einer standardisierten Verwendung von Bildsymbolen in der EU beizutragen, wird der Kommission in der Verordnung die Befugnis übertragen, delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung standardisierter Bildsymbole zu erlassen. Der Europäische Datenschutzausschuss muss eine Stellungnahme zu den von der Kommission vorgeschlagenen Bildsymbolen abgeben. Der Umstand, dass delegierte Rechtsakte erlassen werden können, hindert den Europäischen Datenschutzausschuss nicht daran, Leitlinien, Gutachten und bewährte Verfahren in Bezug auf Bildsymbole herauszugeben.

4.5. Recht auf Zugang

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat die betroffene Person ein Recht auf Zugang zu den in der Verordnung aufgeführten Informationen. In Anbetracht dessen ist in der Verordnung festgelegt, dass der Verantwortliche unentgeltlich eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung stellen muss. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Das Recht auf Erhalt einer Kopie darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

4.6. Recht auf Löschung ("Recht auf Vergessenwerden")

Mit dem Standpunkt des Rates in erster Lesung erhalten betroffene Personen das Recht, zu verlangen, dass sie betreffende personenbezogene Daten gelöscht werden, wenn die Speicherung dieser Daten gegen die Verordnung oder gegen das Recht der Union oder des Mitgliedstaats, dem der Verantwortliche unterliegt, verstößt.

Mit dem Verweis auf das "Recht auf Vergessenwerden" wird eingeräumt, dass das Recht auf Löschung insbesondere im digitalen Kontext angepasst werden muss. Verantwortliche, die die personenbezogenen Daten, deren "Vergessenwerden" die betroffene Person wünscht, öffentlich gemacht haben, müssen geeignete Maßnahmen, auch technischer Art, , um den Verantwortlichen, die die personenbezogenen Daten verarbeiten, mitzuteilen, dass die betroffene Person beantragt hat, dass alle Links zu diesen personenbezogenen Daten oder Kopien oder Replikationen dieser Daten gelöscht werden, wobei die verfügbare Technologie und die Implementierungskosten zu berücksichtigen sind. Der Europäische Datenschutzausschuss kann Leitlinien, Empfehlungen und bewährte Verfahren im Hinblick auf die Verfahren zur Löschung von Links zu personenbezogenen Daten oder von Kopien oder Replikationen solcher Daten aus öffentlich zugänglichen Kommunikationsdiensten bereitstellen.

Das Recht auf Löschung und die dem Verantwortlichen obliegende Pflicht, andere Verantwortliche über einen Antrag auf Löschung zu unterrichten, gelten nicht, soweit die Verarbeitung personenbezogener Daten für die in der Verordnung erschöpfend aufgeführten Zwecke, etwa zur Ausübung des Rechts auf freie Meinungsäußerung und Information, notwendig ist.

4.7. Recht auf Datenübertragbarkeit

Im Standpunkt des Rates in erster Lesung ist festgelegt, dass die betroffenen Personen im Fall einer automatisierten Verarbeitung personenbezogener Daten berechtigt sind, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten und sie einem anderen Verantwortlichen zu übermitteln. Ferner können die betroffenen Personen verlangen, dass die personenbezogenen Daten – soweit technisch machbar – direkt von einem Verantwortlichen an einen anderen Verantwortlichen übermittelt werden. Dies verstärkt die Kontrolle der betroffenen Personen über ihre Daten zusätzlich. Ferner fördert es den Wettbewerb zwischen den Verantwortlichen.

Das Recht auf Datenübertragbarkeit gilt allerdings nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Wenn ferner bei einem bestimmten Satz personenbezogener Daten mehr als eine betroffene Person betroffen ist, gilt das Recht der betroffenen Person, die personenbezogenen Daten zu erhalten, unbeschadet der Rechte und Freiheiten anderer.

4.8. Widerspruchsrecht

In Fällen, in denen die personenbezogenen Daten möglicherweise rechtmäßig verarbeitet werden dürfen, weil die Verarbeitung für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, oder aufgrund des berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist, hat die betroffene Person das Recht, Widerspruch gegen die Verarbeitung der ihre besondere Situation betreffenden personenbezogenen Daten einzulegen. Dann darf der Verantwortliche die personenbezogenen Daten nicht mehr verarbeiten, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

In Anbetracht dessen ist festgelegt, dass, wenn personenbezogene Daten verarbeitet werden, um Direktwerbung zu betreiben, die betroffene Person das Recht hat, jederzeit Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten einzulegen. Dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. Der Begriff "Profiling" ist definiert als jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so dürfen die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet werden. Überdies muss die betroffene Person spätestens zum Zeitpunkt der ersten Kommunikation zwischen dem Verantwortlichen und ihr ausdrücklich und klar auf dieses Recht hingewiesen werden.

Ferner ist im Standpunkt des Rates in erster Lesung ein Verweis auf "Nicht-Verfolgen"-Funktionen enthalten: Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden.

4.9. Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Beispiele hierfür sind die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliches Eingreifen. Diese automatisierte Verarbeitung kann auch das Profiling einschließen. Dieses Recht, nicht einer automatisierten Verarbeitung unterworfen zu werden, gilt nicht, wenn die automatisierte Verarbeitung

– für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist oder

– aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist – wie etwa bei der Überwachung von Betrug und Steuervermeidung – und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

– mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Die Position der betroffenen Person wird ferner dadurch gestärkt, dass der Verantwortliche verpflichtet ist, die betroffene Person, sofern dies notwendig ist, um eine faire und transparente Verarbeitung zu gewährleisten, über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling zu informieren und ihr – zumindest in diesen Fällen – aussagekräftige Informationen über die verwendete Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person bereitzustellen.

Darüber hinaus sind automatisierte Entscheidungsfindung und Profiling auf der Grundlage besonderer Kategorien von personenbezogenen Daten nur unter bestimmten Bedingungen erlaubt, und zwar unter anderem unter Wahrung des Rechts der betroffenen Person, Widerspruch gegen die Weiterverarbeitung dieser personenbezogenen Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken einzulegen, sofern diese nicht zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist.

Der Europäische Datenschutzausschuss kann Leitlinien, Empfehlungen und bewährte Verfahren zur näheren Bestimmung der Kriterien und Bedingungen für die auf Profiling beruhenden Entscheidungen bereitstellen.

5. Verantwortlicher und Auftragsverarbeiter

5.1. Einleitung

Der Standpunkt des Rates in erster Lesung legt den Rechtsrahmen für die Verantwortung und Haftung für die Verarbeitung personenbezogener Daten durch einen Verantwortlichen oder in dessen Namen durch einen Auftragsverarbeiter fest. Im Einklang mit dem Grundsatz der Rechenschaftspflicht muss der Verantwortliche geeignete technische und organisatorische Maßnahmen umsetzen und in der Lage sein, den Nachweis dafür zu erbringen, dass seine Verarbeitungen im Einklang mit der Verordnung erfolgen. Vor diesem Hintergrund enthält die Verordnung Vorschriften über die Verantwortung des Verantwortlichen in Bezug auf Folgenabschätzungen, die Führung eines Verzeichnisses der Verarbeitungstätigkeiten, Verletzungen der Datensicherheit, die Benennung eines Datenschutzbeauftragten sowie über Verhaltenskodizes und Zertifizierungsverfahren.

5.2. Folgenabschätzungen

Der Verantwortliche ist für die Durchführung einer Datenschutz-Folgenabschätzung verantwortlich, mit der evaluiert werden soll, ob die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Der Standpunkt des Rates in erster Lesung legt die Fälle dar, in denen eine besondere Anforderung für eine Datenschutz-Folgenabschätzung besteht, beispielsweise bestimmte umfangreiche Verarbeitungsvorgänge. Geht aus einer solchen Folgenabschätzung hervor, dass Verarbeitungsvorgänge ein hohes Risiko bergen, das der Verantwortliche nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten eindämmen kann, so muss die Aufsichtsbehörde vor der Verarbeitung konsultiert werden. Die Aufsichtsbehörde kann den Verantwortlichen dann beraten und seine Befugnisse ausüben.

Der Europäische Datenschutzausschuss kann Leitlinien für Verarbeitungsvorgänge ausgeben, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten mit sich bringen, und angeben, welche Abhilfemaßnahmen in Bezug auf ein mögliches Risiko ausreichend sein können.

5.3. Verzeichnis von Verarbeitungstätigkeiten

Um Ex-post-Kontrollen durch die Aufsichtsbehörde zu ermöglichen, muss der Verantwortliche oder der etwaige Vertreter des Verantwortlichen oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten führen, die seiner Zuständigkeit unterliegen, einschließlich Verletzungen der Datensicherheit. Um den Verwaltungsaufwand zu verringern, gilt die Aufzeichnungspflicht nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung von sensiblen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten einschließt.

5.4. Verletzungen des Schutzes personenbezogener Daten

Eine Verletzung des Schutzes personenbezogener Daten kann einen physischen, materiellen oder immateriellen Schaden für die betroffenen Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere wirtschaftliche oder gesellschaftliche Nachteile. Der Standpunkt des Rates in erster Lesung sieht vor, dass der Verantwortliche eine Verletzung des Schutzes personenbezogener Daten der Aufsichtsbehörde melden muss, es sei denn, diese Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen. Er muss ferner die betroffenen Personen über solche Verletzungen benachrichtigen, die voraussichtlich ein hohes Risiko bergen. Die Meldung an die Aufsichtsbehörde ermöglicht es dieser, bei Bedarf einzugreifen. Die Benachrichtigung der betroffenen Person ermöglicht es dieser überdies, vorbeugende Maßnahmen zu treffen.

Um den Verwaltungsaufwand zu verringern, werden in dem Standpunkt des Rates in erster Lesung unterschiedliche Schwellenwerte für Meldungen an die Aufsichtsbehörde und für Benachrichtigungen der betroffenen Personen vorgesehen, wobei für Benachrichtigungen ein höherer Schwellenwert gilt als für Meldungen. Der Verantwortliche ist verpflichtet, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die zuständige Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, darüber zu unterrichten. Der Verantwortliche kann die Meldung jedoch unterlassen, wenn er nachweisen kann, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Von einigen Ausnahmen abgesehen, ist der Verantwortliche verpflichtet, die betroffene Person unverzüglich über die Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten dieser Person zur Folge hat.

Der Europäische Datenschutzausschuss kann Leitlinien, Empfehlungen und bewährte Verfahren zur Feststellung von Verletzungen des Schutzes personenbezogener Daten ausgeben, ebenso wie zur Bestimmung, was unter einer unangemessenen Verzögerung nach Kenntnisnahme der Verletzung durch den Verantwortlichen zu verstehen ist, und zu den spezifischen Umständen, unter denen der Verantwortliche die Verletzung des Schutzes personenbezogener Daten zu melden hat, sowie zu den Umständen, unter denen eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

5.5. Datenschutzbeauftragter

Durch die Benennung eines Datenschutzbeauftragten soll die Einhaltung der Verordnung verbessert werden. Der Datenschutzbeauftragte muss infolgedessen über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügen und den Verantwortlichen oder den Auftragsverarbeiter bei der Überwachung der unternehmensinternen Einhaltung dieser Verordnung unterstützen. Er kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen. Ein gemeinsamer Datenschutzbeauftragter kann auch für eine Unternehmensgruppe benannt werden, oder wenn es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde handelt. Der Standpunkt des Rates in erster Lesung sieht die obligatorische Benennung eines Datenschutzbeauftragten vor, wenn

– die Verarbeitung von einer Behörde durchgeführt wird, mit Ausnahme von Gerichten oder unabhängigen Justizbehörden, die im Rahmen ihrer justiziellen Tätigkeit handeln,

– die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

– die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung von sensiblen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht.

5.6. Verhaltensregeln und Zertifizierungsverfahren

Der Standpunkt des Rates in erster Lesung bietet Anreize für die Anwendung von Verhaltensregeln und fördert die umfassendere Verwendung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen. Diese Initiativen tragen zur Einhaltung der Datenschutzvorschriften bei, wobei übermäßig präskriptive Vorschriften vermieden und die Kosten für die für die Durchsetzung zuständigen Behörden verringert werden. Zudem können Verhaltensregeln Besonderheiten der in bestimmten Sektoren erfolgenden Verarbeitungen und die besonderen Bedürfnisse der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen berücksichtigen. Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen tragen ihrerseits zur Einhaltung der Verordnung bei, da die betroffenen Personen das Datenschutzniveau einschlägiger Produkte und Dienstleistungen mühelos beurteilen können.

Der Standpunkt des Rates in erster Lesung enthält ein ausgefeiltes Regelwerk in Bezug auf Verhaltensregeln und Zertifizierungsverfahren, Datenschutzsiegel und -prüfzeichen, die Raum für private Initiativen lassen und gleichzeitig die Datenschutzstandards durch die Beteiligung der Aufsichtsbehörden wahren.

5.6.1. Verhaltensregeln

Die Aufsichtsbehörde kann Verhaltenskodizes beziehungsweise Änderungen oder Erweiterungen solcher Verhaltenskodizes genehmigen. Bezieht sich der Entwurf von Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten, so muss die zuständige Aufsichtsbehörde einen Entwurf von Verhaltensregeln oder von deren Änderung oder Erweiterung dem Europäischen Datenschutzausschuss zur Stellungnahme vorlegen, bevor sie ihn genehmigt.

Die Kommission kann im Wege von Durchführungsrechtsakten beschließen, dass neue Verhaltensregeln beziehungsweise Änderungen oder Erweiterungen bestehender, von der zuständigen Aufsichtsbehörde genehmigter Verhaltensregeln allgemeine Gültigkeit in der Union besitzen.

Der Europäische Datenschutzausschuss sollte die Ausarbeitung von Verhaltensregeln fördern. Er muss auch alle genehmigten Verhaltensregeln oder deren genehmigte Änderungen in ein Register aufnehmen und in geeigneter Weise veröffentlichen.

5.6.2. Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen

Der Standpunkt des Rates in erster Lesung sieht vor, dass alle Mitgliedstaaten mitteilen müssen, ob die Zertifizierungsstellen von der Aufsichtsbehörde oder von der nationalen Akkreditierungsstelle akkreditiert werden. Akkreditierte Zertifizierungsstellen können Verantwortliche und Auftragsverarbeiter auf der Grundlage der Kriterien zertifizieren, die von der zuständigen Aufsichtsbehörde oder im Einklang mit dem Kohärenzverfahren vom Europäischen Datenschutzausschuss genehmigt wurden. Im letzteren Fall können die vom Europäischen Datenschutzausschuss genehmigten Kriterien zu einer gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führen. Die Zertifizierung wird einem Verantwortlichen oder einem Auftragsverarbeiter für eine Höchstdauer von drei Jahren erteilt und kann verlängert werden. Die Zertifizierungsstelle muss der Aufsichtsbehörde die Gründe für die Erteilung oder den Widerruf der beantragten Zertifizierung mitteilen. Anschließend kann die Aufsichtsbehörde eine solche Zertifizierung ablehnen oder für ungültig erklären.

Der Kommission obliegt es, delegierte Rechtsakte zu erlassen, um die Anforderungen festzulegen, die für die datenschutzspezifischen Zertifizierungsverfahren zu berücksichtigen sind. Der Europäische Datenschutzausschuss muss eine Stellungnahme zu diesen Anforderungen abgeben. Die Kommission kann auch Durchführungsrechtsakte zu den technischen Standards für Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen sowie zu den Mechanismen zur Förderung und Anerkennung von Zertifizierungsverfahren und Datenschutzsiegeln und -prüfzeichen erlassen.

Schließlich sollte der Europäische Datenschutzausschuss die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen fördern.

6. Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen

6.1. Einleitung

Der grenzüberschreitende Fluss personenbezogener Daten aus Drittländern und von internationalen Organisationen sowie in Drittländer und an internationale Organisationen ist in einem Kontext des Welthandels und der grenzüberschreitenden digitalen Wirtschaft von entscheidender Bedeutung. Das durch die Union garantierte Schutzniveau darf nicht beeinträchtigt werden, wenn personenbezogene Daten von EU-Bürgern in Gebiete außerhalb der Union übermittelt werden.

Als allgemeiner Grundsatz gilt, dass jedwede Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation nur zulässig ist, wenn der Verantwortliche und der Auftragsverarbeiter die Bestimmungen dieser Verordnung einhalten. Der Standpunkt des Rates in erster Lesung trägt der Rechtsprechung des Gerichtshofs der Europäischen Union, einschließlich des Urteils vom 6. Oktober 2015 in der Rechtssache C-362/14, uneingeschränkt Rechnung. Der Standpunkt des Rates behält die verschiedenen Möglichkeiten für die grenzüberschreitende Übermittlung personenbezogener Daten bei, während gleichzeitig die Garantien, dass Datenschutzrechte gewahrt werden, gestärkt werden. Diese unterschiedlichen Möglichkeiten der Übermittlung personenbezogener Daten erfolgen auf der Grundlage von Angemessenheitsbeschlüssen, geeigneten Garantien und Ausnahmeregelungen.

Im Standpunkt des Rates in erster Lesung wird präzisiert, dass Entscheidungen eines Gerichts eines Drittlands und Entscheidungen einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Weitergabe personenbezogener Daten verlangt wird, jedenfalls nur dann anerkannt oder vollstreckbar werden dürfen, wenn sie auf eine in Kraft befindliche internationale Übereinkunft zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind. Im Standpunkt des Rates in erster Lesung wird überdies ausdrücklich klargestellt, dass solche internationalen Übereinkünfte die anderen Gründe für grenzüberschreitende Übermittlungen gemäß dieser Verordnung unberührt lassen.

6.2. Angemessenheitsbeschlüsse

Internationale Übermittlungen dürfen auf der Grundlage eines Angemessenheitsbeschlusses der Kommission vorgenommen werden, wonach das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein Schutzniveau bietet, das im Wesentlichen dem in der Union garantierten Niveau entspricht. Dadurch wird in der gesamten Union Rechtssicherheit geschaffen und eine einheitliche Rechtsanwendung sichergestellt.

Die Kommission kann nach Übermittlung einer entsprechenden Benachrichtigung und einer umfassenden Begründung an das Drittland oder die internationale Organisation den Widerruf eines Angemessenheitsbeschlusses beschließen. Die Kommission erlässt Angemessenheitsbeschlüsse und Beschlüsse über deren Widerruf in Form von Durchführungsrechtsakten. In den Durchführungsrechtsakten ist ein Mechanismus für eine regelmäßige Überprüfung, die mindestens alle vier Jahre erfolgt, vorzusehen. Die Kommission muss die Entwicklungen in Drittländern und bei internationalen Organisationen überwachen, die die Wirkungsweise der Angemessenheitsbeschlüsse beeinträchtigen könnten. Für die Zwecke der Überwachung und der Durchführung der regelmäßigen Überprüfungen sollte die Kommission die Standpunkte und Feststellungen des Europäischen Parlaments und des Rates sowie der anderen einschlägigen Stellen und Quellen berücksichtigen. Im Rahmen der Bewertung und Überarbeitung der Verordnung muss die Kommission außerdem dem Rat und dem Europäischen Parlament regelmäßig Bericht erstatten. Schließlich muss der Europäische Datenschutzausschuss der Kommission eine Stellungnahme vorlegen, in der die Angemessenheit des Schutzniveaus in einem Drittland oder einer internationalen Organisation beurteilt wird, einschließlich der Prüfung, ob ein angemessenes Schutzniveau nicht mehr gewährleistet ist.

Von der Kommission auf der Grundlage von Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie durch einen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden. In diesem Sinne bleiben von einem Mitgliedstaat oder einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilte Genehmigungen und von der Kommission auf der Grundlage von Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassene Feststellungen so lange gültig, bis sie erforderlichenfalls von der Aufsichtsbehörde oder durch einen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden. Durch Gewährleistung der Kontinuität sorgt der Standpunkt des Rates in erster Lesung für Rechtssicherheit.

6.3. Geeignete Garantien

Zusätzlich zu Angemessenheitsbeschlüssen können grenzüberschreitende Übermittlungen auch stattfinden, wenn der Verantwortliche oder der Auftragsverarbeiter als Ausgleich für den fehlenden Datenschutz in dem Drittland oder der internationalen Organisation geeignete Garantien vorgesehen hat. Diese Garantien können in Folgendem bestehen: rechtlich bindenden und durchsetzbaren Dokumenten zwischen den Behörden oder öffentlichen Stellen, verbindlichen internen Datenschutzvorschriften, von der Kommission erlassenen oder von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln oder von einer Aufsichtsbehörde genehmigten Vertragsklauseln. Verantwortliche oder Auftragsverarbeiter in einem Drittland können auch geeignete Garantien für die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen bereitstellen. Dazu können sie auf genehmigte Verhaltensregeln zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen zur Anwendung der geeigneten Garantien mittels vertraglicher oder sonstiger rechtsverbindlicher Instrumente, einschließlich in Bezug auf die Rechte der betroffenen Personen, zurückgreifen. Sie können dazu auch auf einen von der zuständigen Aufsichtsbehörde genehmigten Zertifizierungsmechanismus zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, zurückgreifen.

6.4. Ausnahmeregelungen

Falls weder ein Angemessenheitsbeschluss vorliegt noch geeignete Garantien bestehen, kann eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation auf der Grundlage von Ausnahmeregelungen stattfinden, die in der Verordnung erschöpfend aufgeführt sind. Eine dieser Ausnahmeregelungen betrifft die berechtigten Interessen des Verantwortlichen, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen. Im Hinblick auf ausreichende Garantien für die grenzüberschreitende Übermittlung von personenbezogenen Daten sind die berechtigten Interessen des Verantwortlichen streng geregelt und dürfen nur als letztes Mittel geltend gemacht werden. Im Hinblick auf die Gewährleistung einer einheitlichen Anwendung der Verordnung muss der Europäische Datenschutzausschuss von sich aus oder auf Ersuchen der Kommission Leitlinien, Empfehlungen und bewährte Praktiken zum Zwecke der weiteren Festlegung der Kriterien und Bedingungen für die Übermittlung von Daten ausarbeiten bzw. überarbeiten, wenn weder ein Angemessenheitsbeschluss vorliegt noch geeignete Garantien bestehen.

7. Aufsichtsbehörden

7.1. Unabhängigkeit

Damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird, muss jeder Mitgliedstaat vorsehen, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung in seinem Hoheitsgebiet zuständig sind. Jede Aufsichtsbehörde und ihre Mitglieder müssen bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse völlig unabhängig und auch integer handeln.

Jede Aufsichtsbehörde muss einen Beitrag zur einheitlichen Anwendung der Verordnung in der gesamten Union leisten. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden untereinander sowie mit dem Europäischen Datenschutzausschuss und der Kommission. Die einheitliche Anwendung der Verordnung wird zudem dadurch gewährleistet, dass die Zuständigkeiten der Aufsichtsbehörden geregelt und die Aufgaben und Untersuchungs-, Abhilfe- und Genehmigungsbefugnisse sowie beratenden Befugnisse, über die die Aufsichtsbehörden mindestens verfügen müssen, festgelegt werden.

7.2. Verschwiegenheitspflicht

Im Standpunkt des Rates in erster Lesung werden Vorschriften über die Verschwiegenheitspflicht der Aufsichtsbehörden und ihrer Mitglieder festgelegt. Zunächst einmal sind das Mitglied oder die Mitglieder und die Bediensteten jeder Aufsichtsbehörde gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten sowohl während ihrer Amts- bzw. Dienstzeit als auch nach deren Beendigung verpflichtet, über alle vertraulichen Informationen, die ihnen bei der Wahrnehmung ihrer Aufgaben oder der Ausübung ihrer Befugnisse bekannt geworden sind, Verschwiegenheit zu wahren. Ferner wird festgelegt, dass diese Verschwiegenheitspflicht während dieser Amts- bzw. Dienstzeit insbesondere für die von natürlichen Personen gemeldeten Verstöße gegen die Verordnung gilt. Außerdem hat der Europäische Datenschutzausschuss die Aufgabe, Leitlinien, Empfehlungen und bewährte Verfahren zur Festlegung gemeinsamer Verfahren für die von natürlichen Personen vorgenommene Meldung von Verstößen gegen die Verordnung bereitzustellen.

8. Zusammenarbeit und Kohärenz

8.1. Europäischer Datenschutzausschuss

Im Standpunkt des Rates in erster Lesung ist vorgesehen, dass der Europäische Datenschutzausschuss als Einrichtung der Union mit eigener Rechtspersönlichkeit geschaffen wird, um die ordnungsgemäße und einheitliche Anwendung der Verordnung sicherzustellen. Der Ausschuss schaltet sich insbesondere mit Stellungnahmen, verbindlichen Beschlüssen im Zusammenhang mit der Beilegung von Streitigkeiten zwischen Aufsichtsbehörden oder Leitlinien zu Fragen im Zusammenhang mit der Anwendung dieser Verordnung zur Gewährleistung ihrer einheitlichen Durchsetzung ein.

Der Europäische Datenschutzausschuss besteht aus dem Leiter einer Aufsichtsbehörde jedes Mitgliedstaats und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern. Die Kommission ist berechtigt, ohne Stimmrecht an den Tätigkeiten und Sitzungen des Europäischen Datenschutzausschusses teilzunehmen. Die Beratungen des Europäischen Datenschutzausschusses sind gemäß seiner Geschäftsordnung vertraulich, wenn der Ausschuss dies für erforderlich hält.

Erlässt der Europäischen Datenschutzausschuss einen verbindlichen Beschluss im Zusammenhang mit einer Streitbeilegung, ist der Europäische Datenschutzbeauftragte nur bei Beschlüssen stimmberechtigt, die Grundsätze und Vorschriften betreffen, die für die Organe, Einrichtungen, Ämter und Agenturen der Union gelten und inhaltlich den Grundsätzen und Vorschriften dieser Verordnung entsprechen.

8.2. Kohärenzverfahren

In Fällen grenzüberschreitender Verarbeitung personenbezogener Daten, mit denen mehr als eine Aufsichtsbehörde befasst ist, wird mit dem Kohärenzverfahren sichergestellt, dass ein einziger Beschluss gefasst wird, der in der gesamten Europäischen Union gilt, wobei die Standpunkte der verschiedenen betroffenen Aufsichtsbehörden berücksichtigt werden. Mit dem Kohärenzverfahren wird daher durch Einbindung der Aufsichtsbehörden vor Ort in die Entscheidungsfindung eine größere "Nähe" zwischen den betroffenen Personen und der entscheidenden Aufsichtsbehörde geschaffen. Außerdem ist bei Streitigkeiten zwischen Aufsichtsbehörden aus verschiedenen Mitgliedstaaten der neu geschaffene Datenschutzausschuss befugt, verbindliche Beschlüsse zu fassen.

Die Vorschriften über das Kohärenzverfahren finden keine Anwendung, wenn die Verarbeitung durch Behörden oder private Einrichtungen, die im öffentlichen Interesse handeln, erfolgt. In diesen Fällen ist die Aufsichtsbehörde des Mitgliedstaats, in dem die Behörde oder private Einrichtung ihren Sitz hat, die einzige zuständige Aufsichtsbehörde.

Im Standpunkt des Rates in erster Lesung ist vorgesehen, dass im Zusammenhang mit der Bewertung der Verordnung durch die Kommission, die Anwendung des Zusammenarbeits- und Kohärenzverfahrens geprüft wird.

9. Rechtsbehelfe, Haftung und Sanktionen

Im Standpunkt des Rates in erster Lesung wird eine Reihe von Vorschriften festgelegt, mit denen den betroffenen Personen mehrere Möglichkeiten für Rechtsbehelfe geboten werden, so auch die Möglichkeit, bei Schäden infolge von Verstößen gegen die Verordnung Schadensersatz zu verlangen.

9.1. Recht auf Beschwerde und Recht auf gerichtlichen Rechtsbehelf

Im Standpunkt des Rates in erster Lesung ist vorgesehen, dass jede betroffene Person das Recht auf Beschwerde bei einer Aufsichtsbehörde hat, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt. Zudem hat jede betroffene Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde. Falls die Aufsichtsbehörde sich nicht mit der Beschwerde befasst oder keine Informationen über den Stand oder das Ergebnis der erhobenen Beschwerde erteilt hat, hat die betroffene Person ebenfalls das Recht auf einen wirksamen Rechtsbehelf.

Jede betroffene Person hat ferner das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit der Verordnung erfolgenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

Die Nähe zwischen der betroffenen Person und dem nationalen Gericht wird dadurch sichergestellt, dass die betroffenen Personen das Recht auf Überprüfung eines Beschlusses ihrer Datenschutzbehörde durch ihre nationalen Gerichte haben, unabhängig davon, in welchem Mitgliedstaat der Verantwortliche oder der Auftragsverarbeiter niedergelassen ist. Für Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

Schließlich hat jede natürliche oder juristische Person das Recht, unter den in Artikel 263 AEUV genannten Voraussetzungen beim Gerichtshof der Europäischen Union eine Klage auf Nichtigerklärung eines Beschlusses des Europäischen Datenschutzausschusses zu erheben.

9.2. Vertretung von betroffenen Personen

Zudem hat die betroffene Person das Recht, eine Einrichtung, Organisation oder Vereinigung, die bestimmte Kriterien erfüllt, beispielsweise dass sie ohne Gewinnerzielungsabsicht und insbesondere im Bereich des Datenschutzes tätig ist, zu beauftragen, in ihrem Namen eine Beschwerde einzureichen, in ihrem Namen die Rechte auf einen gerichtlichen Rechtsbehelf wahrzunehmen und das Recht auf Schadensersatz in Anspruch zu nehmen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist. Mit diesen spezifischen Kriterien soll die Entwicklung einer Kultur von handelsrechtlichen Klagen im Bereich des Datenschutzes verhindert werden. Darüber hinaus können die Mitgliedstaaten vorsehen, dass jede der genannten Einrichtungen, Organisationen oder Vereinigungen unabhängig von einem Auftrag der betroffenen Person in diesem Mitgliedstaat das Recht hat, bei der zuständigen Aufsichtsbehörde eine Beschwerde einzulegen und die Rechte auf einen gerichtlichen Rechtsbehelf in Anspruch zu nehmen, wenn ihres Erachtens die Rechte einer betroffenen Person infolge einer nicht der Verordnung entsprechenden Datenverarbeitung verletzt worden sind.

9.3. Aussetzung des Verfahrens

Um zu verhindern, dass derselbe Gegenstand in Bezug auf die Verarbeitung durch denselben Verantwortlichen oder Auftragsverarbeiter von verschiedenen Gerichten geprüft wird, kann jedes später angerufene zuständige Gericht das bei ihm anhängige Verfahren aussetzen oder sich auf Antrag einer Partei für unzuständig erklären.

9.4. Haftung und Recht auf Schadensersatz

Im Standpunkt des Rates in erster Lesung ist vorgesehen, dass jede betroffene Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter hat. Um den betroffenen Personen die Möglichkeit zu geben, im Falle eines Schadens Schadensersatz zu verlangen, und den Verantwortlichen und den Auftragsverarbeitern zugleich Rechtssicherheit zu bieten, wird in der Verordnung deren Haftung im Einzelnen festgelegt. Jeder an der Verarbeitung beteiligte Verantwortliche haftet für den durch die Verarbeitung verursachten Schaden. Ein Auftragsverarbeiter haftet nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat. Allerdings wird der Verantwortliche oder der Auftragsverarbeiter von der Haftung befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist. Hat jedoch ein Verantwortlicher oder Auftragsverarbeiter vollständigen Schadensersatz für den erlittenen Schaden gezahlt, so ist der Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten Verantwortlichen oder Auftragsverarbeitern den Teil des Schadensersatzes zurückzufordern, der ihrem Anteil an der Verantwortung für den Schaden entspricht.

9.5. Sanktionen

Um die Einhaltung der Verordnung sicherzustellen, ist im Standpunkt des Rates in erster Lesung vorgesehen, dass die Aufsichtsbehörden Geldbußen verhängen können. Diese Geldbußen müssen wirksam, verhältnismäßig und abschreckend sein. Ein Mitgliedstaat kann Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Einrichtungen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können. Neben der Verhängung von Geldbußen können die Aufsichtsbehörden auch von anderen Abhilfebefugnissen, wie z. B. Warnungen oder Tadeln, Gebrauch machen. Um die Harmonisierung zu verstärken, muss der Europäische Datenschutzausschuss Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung der Abhilfebefugnisse der Aufsichtsbehörden und die Festsetzung von Geldbußen aufstellen.

Der Standpunkt des Rates in erster Lesung enthält eine Liste von Kriterien, die die Aufsichtsbehörden berücksichtigen, wenn sie darüber entscheiden, ob und, wenn ja, in welcher Höhe eine Geldbuße verhängt wird. Diese Kriterien beziehen sich unter anderem auf die Art, Schwere und Dauer bzw. die Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes gegen die Verordnung. In der Verordnung werden sowohl die Verstöße als auch die entsprechenden Höchstbeträge der Geldbußen aufgeführt. Die Aufsichtsbehörden müssen unter Beachtung des Höchstbetrags der Geldbuße je nach den Umständen des einzelnen Verstoßes einen angemessen Betrag festlegen. Um den Verantwortlichen und den Auftragsverarbeitern Rechtssicherheit zu bieten und die Harmonisierung der Geldbußen innerhalb der Union zu verstärken und gleichzeitig den Aufsichtsbehörden einen Ermessensspielraum einzuräumen, sind diese Verstöße in drei Kategorien unterteilt: Bei Verstößen der ersten Kategorie, die die Pflichten der Verantwortlichen und der Auftragsverarbeiter betreffen, können Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist. Bei Verstößen der zweiten Kategorie, d.h. Verstößen gegen die Rechte der betroffenen Personen und die allgemeinen Grundsätze, liegt die Obergrenze bei 20 000 000 EUR bzw. 4 % des Jahresumsatzes. Verstöße der dritten Kategorie betreffen die Nichtbefolgung einer Anweisung der Aufsichtsbehörde und sind ebenfalls mit einer Geldbuße von bis zu 20 000 000 EUR bzw. 4 % des Jahresumsatzes bedroht.

10. Besondere Datenverarbeitungssituationen

10.1. Verarbeitung personenbezogener Daten und Freiheit der Meinungsäußerung und Informationsfreiheit

Die Mitgliedstaaten bringen durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung personenbezogener Daten zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken, in Einklang. Um die Transparenz hinsichtlich der Übereinstimmung dieser Rechte zu gewährleisten, ist jeder Mitgliedstaat verpflichtet, der Kommission seine einschlägigen Rechtsvorschriften und deren Änderungen sowie neue einschlägige Vorschriften mitzuteilen.

10.2. Datenverarbeitung im Beschäftigungskontext

Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen.

Diese Vorschriften umfassen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person. Jeder Mitgliedstaat muss der Kommission die einschlägigen Rechtsvorschriften und deren Änderungen sowie neue einschlägige Vorschriften mitteilen.

10.3. Garantien und Ausnahmen in Bezug auf die Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

Im Standpunkt des Rates in erster Lesung werden spezifische Vorschriften für die Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken festgelegt. Mit diesen Vorschriften soll das Interesse an der Verfügbarkeit von personenbezogenen Daten, die dazu dienen, Archive zu führen, Statistiken zu erstellen und Forschung zu betreiben, mit den Datenschutzrechten in Einklang gebracht werden.

Die Verarbeitung personenbezogener Daten für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken muss geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß der Verordnung unterliegen. Es ist den Mitgliedstaaten erlaubt, unter bestimmten Bedingungen und vorbehaltlich geeigneter Garantien für die betroffenen Personen Präzisierungen und Ausnahmen in Bezug auf die Informationsanforderungen sowie die Rechte auf Berichtigung, Löschung, Vergessenwerden, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch vorzusehen, wenn personenbezogene Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet werden.

Der Standpunkt des Rates in erster Lesung gestattet auch Ausnahmen vom Verbot der Verarbeitung sensibler personenbezogener Daten, wenn die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken erfolgt. Eine derartige Ausnahme ist gestattet, wenn sich die Verarbeitung auf Rechtsvorschriften der Union oder der Mitgliedstaaten stützt, die in einem angemessenen Verhältnis zu dem verfolgten Ziel stehen, den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen.

11. Bereits geschlossene Übereinkünfte

Im Standpunkt des Rates in erster Lesung ist festgelegt, dass internationale Übereinkünfte, die die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen mit sich bringen, die von den Mitgliedstaaten vor dem Inkrafttreten dieser Verordnung abgeschlossen wurden und die im Einklang mit dem vor Inkrafttreten dieser Verordnung geltenden Unionsrecht stehen, in Kraft bleiben, bis sie geändert, ersetzt oder gekündigt werden. Dies gewährleistet Rechtssicherheit für die für die Verarbeitung Verantwortlichen und verhindert unnötigen Verwaltungsaufwand für die Mitgliedstaaten. Außerdem wird dadurch berücksichtigt, dass die Mitgliedstaaten für die Änderung geltender Übereinkünfte auf die Kooperationsbereitschaft von Drittstaaten oder internationalen Organisationen angewiesen sind.

IV. FAZIT

Der Standpunkt des Rates in erster Lesung spiegelt den in den informellen Verhandlungen zwischen dem Rat und dem Europäischen Parlament erzielten Kompromiss wider, der mit Hilfe der Kommission zustande gekommen ist. Der Rat ersucht das Europäische Parlament, den Standpunkt des Rates in erster Lesung ohne Abänderungen förmlich anzunehmen, damit der neue EU-Rechtsrahmen für den Datenschutz, mit dem die Datenschutzrechte gestärkt werden und gleichzeitig der Verkehr personenbezogener Daten im digitalen Markt erleichtert wird, festgelegt werden kann.