RAT DER EUROPÄISCHEN UNION

Brüssel, den 28. Februar 2014 (OR. en)

6762/1/14 REV 1

Interinstitutionelles Dossier: 2012/0011 (COD)

DATAPROTECT 30
JAI 102
MI 191
DRS 26
DAPIX 25
FREMP 28
COMIX 110
CODEC 503

VERMERK

des	Vorsitzes
für den	Rat
Nr. Vordok.:	17831/13 DATAPROTECT 201 JAI 1149 MI 1166 DRS 223 DAPIX 158 FREMP 209 COMIX 700 CODEC 2973 5879/14 DATAPROTECT 13 JAI 46 MI 91 DRS 14 DAPIX 7 FREMP 12 COMIX 68 CODEC 230 5881/14 DATAPROTECT 15 JAI 48 MI 93 DRS 16 DAPIX 9 FREMP 14 COMIX 70 CODEC 232 5344/1/14 REV 1 DATAPROTECT 4 JAI 22 MI 38 DRS 7 DAPIX 4 FREMP 4 COMIX 28 CODEC 91
Betr.:	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) [erste Lesung] – Orientierungsaussprache über bestimmte Punkte

I. Einleitung

1. Der Rat betrachtet das von der Kommission am 25. Januar 2012 vorgelegte Datenschutz-Reformpaket als Angelegenheit höchster Priorität und behandelt es vorrangig. Das Datenschutz-Reformpaket umfasst zwei Gesetzgebungsvorschläge, die sich auf Artikel 16 AEUV stützen. Mit dem ersten Vorschlag für eine Datenschutz-Grundverordnung soll die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ersetzt werden. Der zweite Vorschlag betrifft eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, die an die Stelle des Rahmenbeschlusses 2008/977/JI vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, treten soll.

2. Der Europäische Rat hat auf seiner Tagung vom 24./25. Oktober 2013, in deren Mittelpunkt die Themen digitale Wirtschaft, Innovation und Dienstleistungen standen, abschließend festgestellt, dass "[d]ie rechtzeitige Verabschiedung eines soliden allgemeinen Rahmens für den Datenschutz in der EU und der Cybersicherheitsrichtlinie für die Vollendung des digitalen Binnenmarkts bis 2015 von entscheidender Bedeutung [ist]".

3. Der Vorsitz hat in den ersten beiden Monaten seiner Amtszeit bestimmte wichtige Aspekte der Reform eingehend erörtert, wobei er sich auf die Arbeiten des dänischen, des zyprischen, des irischen und des litauischen Vorsitzes gestützt hat. Er hat dem Legislativpaket zum Datenschutz (Verordnung und Richtlinie) mehr als zehn ganztägige Sitzungen gewidmet.

4. Die Justizminister haben bei informellen Gesprächen, die sie in Athen am 23./24. Januar 2014 geführt haben, die Bestimmungen des Verordnungsentwurfs hinsichtlich internationaler Aspekte als allgemein zufriedenstellend bezeichnet und sich dafür ausgesprochen, diese Modelle gegebenenfalls durch weitere alternative Modelle zu erweitern. Derartige Bestimmungen sind in der heutigen globalisierten Welt der Garant für die Aufrechterhaltung des umfassenden Schutzes, den EU-Bürger genießen, wenn sie zum Ziel von außerhalb der EU niedergelassenen Unternehmen werden und wenn ihre personenbezogenen Daten an Drittstaaten oder internationale Organisationen weitergegeben werden.

5. Die Datenschutz-Grundverordnung baut auf dem bewährten System und den Grundsätzen der Datenschutzrichtlinie (Richtlinie 95/46/EG) auf. Die Kommission kann im Rahmen des Ausschussverfahrens unter Einbeziehung sowohl der Vertreter der Mitgliedstaaten als auch des Europäischen Parlaments durch Beschluss feststellen, ob ein Drittland beziehungsweise bestimmte Gebiete oder Verarbeitungssektoren eines Drittlands oder eine internationale Organisation einen angemessenen Schutz bietet. Der Europäische Datenschutzausschuss wird nach seiner Anhörung eine Stellungnahme abgeben. Einer der von der Kommission erlassenen Angemessenheitsbeschlüsse betrifft die Datenübermittlung zu kommerziellen Zwecken zwischen der EU und den Vereinigten Staaten (Entscheidung 2000/250/EG der Kommission zu "safe harbour", d.h. dem Grundsatz des "sicheren Hafens"). Die Kommission hat im November 2013 eine Mitteilung zum Thema "Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA" vorgelegt und führt derzeit intensive Gespräche mit der US-Seite über das Safe-Harbour-System mit dem Ziel, dieses bis zum Sommer zu verstärken.

6. Der Verordnungsentwurf sieht zudem vor, dass Datenübermittlungen an Drittländer zulässig sind, wenn der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter geeignete Garantien, einschließlich auf der Grundlage unternehmensinterner Datenschutzvorschriften und Vertragsklauseln, vorgesehen hat. Die Rolle der genehmigten Verhaltensregeln und der genehmigten Zertifizierungsverfahren wurde verstärkt. Übermittlungen dieser Art sollten jenen gleichgestellt werden, die sich auf Angemessenheitsbeschlüsse stützen. Übermittlungen sind auch gemäß den begrenzten Ausnahmen, die für Sonderfälle vorgesehen sind, zulässig.

7. Auf der Grundlage der Ergebnisse der Ratstagung vom Juni 2013 hat die Gruppe "Informationsaustausch und Datenschutz" (DAPIX) bestimmte Aspekte der Kapitel I bis IV einer weiteren Prüfung unterzogen. Es wurde eingehend über das Recht auf Datenübertragbarkeit und die Erstellung von Profilen sowie über die Pseudonymisierung und die Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter beraten. Im Anschluss an diese Beratungen hat der Vorsitz bestimmte Punkte der Kapitel I bis IV weiter umformuliert.

8. Der Vorsitz fügt Textvorschläge zum räumlichen Geltungsbereich, zu Kapitel V (Internationale Datenübermittlungen) und zu wichtigen Punkten der Kapitel I bis IV, wie oben dargelegt, (...) bei. Der in den Anlagen I und II enthaltene Text entspricht dem Ergebnis der Beratungen unter dem dänischen, dem zyprischen, dem irischen, dem litauischen und dem hellenischen Vorsitz.

9. Unter hellenischem Vorsitz sind erhebliche weitere Fortschritte bei den Verhandlungen über diesen Verordnungsentwurf erzielt worden. Die Beratungen über das Prinzip der zentralen Kontaktstelle werden auf der Grundlage der Angaben fortgesetzt, die die Minister auf den Tagungen des Rates (Justiz und Inneres) im Oktober und Dezember 2013 erteilt haben.

II. Räumlicher Geltungsbereich und Kernprinzipien für internationale Übermittlungen

10. Während der informellen Gespräche, die im Januar 2014 in Athen geführt worden sind, haben die Minister ihre allgemeine Zufriedenheit mit den Bestimmungen des Verordnungsentwurfs betreffend internationale Übermittlungen und den räumlichen Geltungsbereich der Verordnung zum Ausdruck gebracht, wobei sie die Notwendigkeit hervorhoben, weitgehend sicherzustellen, dass nicht in der Union niedergelassene für die Verarbeitung Verantwortliche den Unionsvorschriften unterliegen, wenn sie personenbezogene Daten von in der Union ansässigen Personen verarbeiten.

    Zudem betonten die Minister, dass die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen auf der Grundlage von Ausnahmen (d.h. nicht auf der Grundlage der Feststellung, dass geeignete/angemessene Garantien – einschließlich unternehmensinterner Datenschutzvorschriften und Vertragsklauseln – bestehen) als Ausnahmefall zu betrachten ist und dass es Garantien bedarf, um die Einhaltung der in Artikel 8 der EU-Grundrechtecharta verankerten Grundrechte und -freiheiten im Hinblick auf den Schutz personenbezogener Daten sicherzustellen.

    Hinsichtlich etwaiger künftiger neuer Modelle (Alternativen) für die internationale Datenübermittlung ist der Vorsitz der Auffassung, dass diese Modelle der Logik des derzeit vorgeschlagenen – vielseitigen aber kohärenten – Systems folgen können bzw. sollten, <u>das auf Übermittlungen auf der Grundlage von Angemessenheitsfeststellungen, angemessenen Garantien und Ausnahmeregelungen basiert</u> und dem die Minister <u>während der informellen Gespräche in Athen</u> ihre Zustimmung erteilt haben. Der vorliegende Kompromiss ist zukunftssicher und bietet genügend Ausweitungsmöglichkeiten auf neue Modelle, die sich auf angemessene Garantien stützen und somit den Schutz der Personen garantieren, deren Daten international übermittelt werden.

III. Zentrale Bestimmungen – Kapitel I bis IV

Die vier zu erörternden Themen greifen einige der wichtigsten technologischen Entwicklungen der letzten Jahre auf. In jedem dieser Fälle ist der Vorsitz bestrebt, dafür zu sorgen, dass sich das volle Potenzial der vorgeschlagenen Verordnung in einer Weise entfaltet, die das Vertrauen in den digitalen Binnenmarkt fördert.

Pseudonymisierung

11. Die Pseudonymisierung personenbezogener Daten ist ein gewöhnlicher Vorgang in der digitalen Welt und zählt zu den wichtigsten Datenschutzvorkehrungen im Rahmen eines risikobasierten Ansatzes. Daher sollte die Pseudonymisierung gefördert werden, wobei derartige Daten jedoch personenbezogene Daten bleiben. Die Beratungen auf fachlicher Ebene haben dazu geführt, dass die "Pseudonymisierung" in die Verordnung aufgenommen wurde, um die Beeinträchtigung der individuellen Rechte einzuschränken und die Datensicherheit zu verstärken. Sie wird dazu beitragen, ein ausgewogenes Verhältnis zwischen dem Schutz der Grundrechte und -freiheiten der betroffenen Personen und der im öffentlichen und privaten Sektor erforderlichen Verarbeitung großer Datenmengen herzustellen. Die Pseudonymisierung kann durch folgendes Beispiel veranschaulicht werden: Medizinische Daten krebskranker Patienten werden dahin gehend bereinigt, dass sämtliche die Patienten unmittelbar identifizierenden Angaben, z.B. Namen, gelöscht werden und jedem Patienten nach dem Zufallsprinzip eine laufende Nummer zugeteilt wird, damit die Informationen anschließend für die medizinische Forschung oder für Zwecke der öffentlichen Gesundheit verwendet werden können.

Übertragbarkeit personenbezogener Daten

12. Ziel der Übertragbarkeit der personenbezogenen Daten ist es, den betroffenen Personen die Möglichkeit zu geben, ihre eigenen Daten von einem Diensteanbieter zu einem anderen zu überführen, wenn sie sich für einen Wechsel des Anbieters entschieden haben (z.B. im Fall der Übertragung der Daten über ihre berufliche Laufbahn von einem allgemeinen sozialen Netzwerk zu einem professionellen berufsorientierten Netzwerk). Diese Beratungen haben gezeigt, wie wichtig das Recht auf Übertragbarkeit der Daten ist, um den Bürgern die Kontrolle über ihre Daten – insbesondere im Internet – zu geben und den aktuellen Rahmen zu modernisieren. Der Vorsitz hat den Anliegen einiger Delegationen Rechnung getragen, indem er den öffentlichen Sektor aus dem Geltungsbereich dieses Rechts ausgeschlossen hat und indem er den Geltungsbereich näher bestimmt hat, damit die für die Datenverarbeitung Verantwortlichen nicht überlastet werden. Der Kompromiss gewährleistet den Schutz anderer betroffener Personen und trägt der Notwendigkeit Rechnung, die technologische Neutralität zu wahren.

Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter

13. Heutzutage haben Diensteanbieter eine weitaus wichtigere Rolle in der digitalen Wirtschaft als im Jahr 1995. Neue technologische Entwicklungen, insbesondere das Cloud-Computing, erfordern eine Verbesserung und Klärung der Rolle und der Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter (einschließlich Sub-Auftragsverarbeiter) bei der Datenverarbeitung. Der Vorsitz hat sich darum bemüht, die Beziehung zwischen den für die Verarbeitung Verantwortlichen und den Auftragsverarbeitern zu klären, einschließlich durch die Aufnahme einer Bezugnahme auf fakultative "standardisierte" Verträge zwischen für die Verarbeitung Verantwortlichen und Auftragsverarbeitern. Beratungen auf fachlicher Ebene haben gezeigt, dass dies befürwortet wird.

Auf Profiling basierende automatisierte Entscheidungsprozesse

13. Die Verarbeitung personenbezogener Daten ist für eine wissensbasierte Wirtschaft absolut unerlässlich. Im digitalen Zeitalter beruhen zahlreiche Wirtschaftstätigkeiten auf der Erstellung und Nutzung bestimmter Profile. So stützt sich die Internet-Werbung, die ihrerseits ein wichtiges wirtschaftliches Fundament des Internet bildet, oftmals auf die Erstellung und Nutzung bestimmter Profile für Marketingzwecke. Die Erstellung und Nutzung von Kundenprofilen kann auch zum Schutz der Kunden, beispielsweise vor Kreditkartenbetrug oder anderen Formen des Betrugs in der digitalen Umgebung, verwendet werden.

Allerdings könnte eine Verarbeitung, die dazu dient, Aspekte zu bewerten (d.h zu analysieren und prognostizieren), die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen (Profiling), die Rechte und Freiheiten der Personen ernsthaft gefährden. Die Richtlinie aus dem Jahr 1995 räumt bereits jeder Person das Recht ein (Artikel 15), keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke einiger der obengenannten Aspekte ergeht. Unter derartige Entscheidungen könnten Handlungen wie beispielsweise die ohne menschliches Eingreifen erfolgende automatische Verweigerung eines Online-Kreditantrags fallen. Diese Vorschrift soll somit in erster Linie verhindern, dass natürliche Personen Entscheidungen unterworfen werden, die im Zuge eines automatisierten Vorgangs ohne menschliches Eingreifen ergehen.

Der vorliegende Kompromiss führt kein spezielles Regelwerk für Profiling-Tätigkeiten als solche ein. Er unterwirft diese Tätigkeiten den allgemeinen Regelungen für die Verarbeitung personenbezogener Daten (Rechtsgrundlagen für die Datenverarbeitung, Grundsätze des Datenschutzes), die mit besonderen Garantien (beispielsweise die Verpflichtung zur Durchführung einer Folgenabschätzung in bestimmten Fällen – Artikel 33 und 34) oder Vorschriften über die Unterrichtung der betroffenen Person einhergehen. Der Europäische Datenschutzausschuss würde die Möglichkeit haben, Leitlinien diesbezüglich herauszugeben.

Der Vorsitz beabsichtigt, dafür zu sorgen, dass natürliche Personen nicht einer allein auf einer automatisierten Verarbeitung, einschließlich auf Profiling basierenden Entscheidung unterworfen werden, die ihnen gegenüber rechtliche Wirkung entfaltet oder sie erheblich beeinträchtigt.

Der vorliegende Text zielt darauf ab, auf einem automatisierten Verarbeitungsvorgang – nämlich (aber nicht ausschließlich) dem Profiling – basierende Entscheidungen zu verbieten, nicht jedoch die Erstellung und Nutzung von Profilen an sich.

Automatisierte Entscheidungsprozesse, die für den Abschluss oder die Erfüllung eines Vertrags erforderlich sind, sollten zulässig sein, sofern die betroffene Person ihre ausdrückliche Einwilligung erteilt hat oder sie nach dem Unionsrecht und dem Recht der Mitgliedstaaten ausdrücklich erlaubt sind, auch zum Zwecke der Vorbeugung von Betrug und Steuerhinterziehung und zum Zwecke der Überwachung.

Profiling oder automatisierte Entscheidungen unter Zugrundelegung besonderer Kategorien von personenbezogenen Daten sollten nur unter bestimmten Bedingungen erlaubt sein.

IV. Fragen

Der Vorsitz ist sich bewusst, dass eine Befürwortung eines Aspekts immer unter Vorbehalt erfolgt, da kein Teil des Verordnungsentwurfs endgültig festgelegt werden kann, solange kein Einvernehmen über den gesamten Wortlaut der Verordnung erzielt worden ist.

In Anbetracht dessen wird der Rat ersucht,

A. *zu erörtern, ob der Rat im Anschluss an die Beratungen auf der informellen Ministertagung in Athen seine breite Unterstützung für den Entwurf von Vorschriften über den räumlichen Anwendungsbereich der Verordnung (Artikel 3 Absatz 2) (siehe Anlage I) bestätigt;*

B. *zu erörtern, ob der Rat im Anschluss an die Beratungen auf der informellen Ratstagung in Athen bestätigt, dass seine Verständigung über die Kernprinzipien des Kapitels V (Anlage II) als Grundlage für die abschließende fachliche Beratung dieses Kapitels durch die Gruppe "Informationsaustausch und Datenschutz" (DAPIX) dient;*

C. *zu bestätigen, dass die Gruppe "Informationsaustausch und Datenschutz" (DAPIX) ihre Arbeit auf der Grundlage der bisher erzielten Fortschritte fortsetzen und die Beratungen zu folgenden Punkten zum Abschluss bringen sollte:*

1) *Pseudonymisierung als Element eines risikobasierten Ansatzes (siehe Anlage III);*
2) *Übertragbarkeit personenbezogener Daten für den Privatsektor (siehe Anlage IV);*
3) *Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter (siehe Anlage V);*

D. *zu erörtern, ob der Verordnungsentwurf, wie auch die Richtlinie 95/46/EG,*

a. *lediglich die automatisierten Entscheidungsprozesse, die insbesondere (aber nicht ausschließlich) auf Profilen basieren und die gegenüber natürlichen Personen rechtliche Wirkung entfalten oder diese erheblich beeinträchtigen, regulieren sollte, oder*
b. *ob die Verordnung auch eine besondere Regelung für die Erstellung und Nutzung von Profilen vorsehen sollte.*

_____

RÄUMLICHER ANWENDUNGSBEREICH

(19) Jede Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union sollte gemäß dieser Verordnung erfolgen, gleich, ob die Verarbeitung in oder außerhalb der Union stattfindet. Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich.

(20) Um sicherzugehen, dass Personen nicht des Schutzes beraubt werden, auf den sie nach dieser Verordnung ein Anrecht haben, sollte die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen dieser Verordnung unterliegen, wenn die Verarbeitung dazu dient, diesen Personen gegen Entgelt oder unentgeltlich Waren oder Dienstleistungen **(...)** in der Union anzubieten. Um festzustellen, ob ein für die Verarbeitung Verantwortlicher diesen betroffenen Personen in der Union Waren oder Dienstleistungen anbietet, sollte geprüft werden, ob er offensichtlich beabsichtigt, Geschäfte mit in einem oder mehreren Mitgliedstaaten der Union ansässigen betroffenen Personen zu tätigen. Während die bloße Zugänglichkeit der Website eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union oder einer E-Mail-Adresse oder anderer Kontaktdaten, oder die Verwendung einer Sprache, die in dem Drittland, in dem der für die Verarbeitung Verantwortliche niedergelassen ist, allgemein gebräuchlich ist, hierfür kein ausreichender Anhaltspunkt ist, können andere Faktoren, wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen, und/oder die Erwähnung von in der Union ansässigen Kunden oder Nutzern darauf hindeuten, dass der für die Verarbeitung Verantwortliche beabsichtigt, diesen betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten **(...)**.

(21) Die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen sollte auch dann dieser Verordnung unterliegen, wenn sie dazu dient, das Verhalten dieser Personen in der Europäischen Union zu beobachten. Ob eine Verarbeitungstätigkeit der Beobachtung des Verhaltens von Personen gilt, sollte daran festgemacht werden, ob ihre Internetaktivitäten mit Hilfe von Datenverarbeitungstechniken nachvollzogen werden, durch die von einer Person ein Profil erstellt wird, das die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen.

(22) Ist nach internationalem Recht das innerstaatliche Recht eines Mitgliedstaats anwendbar, z.B. in einer diplomatischen oder konsularischen Vertretung eines Mitgliedstaats, sollte die Verordnung auch auf einen nicht in der EU niedergelassenen für die Verarbeitung Verantwortlichen Anwendung finden.

Artikel 3

Räumlicher Anwendungsbereich

1. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt.

2. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen, wenn die Datenverarbeitung
   a) dazu dient, diesen Personen Waren oder Dienstleistungen in der Union anzubieten, unabhängig davon, ob von der betroffenen Person eine Zahlung zu leisten ist;
   b) der Beobachtung ihres Verhaltens dient, soweit ihr Verhalten in der Europäischen Union erfolgt.

3. Diese Verordnung findet Anwendung auf jede Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen an einem Ort, der nach internationalem Recht dem Recht eines Mitgliedstaats unterliegt.

ANNEX II

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

78) Cross-border flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to **recipients in** third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to **recipients in** another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer may only take place if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller or processor.

79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects.

80) The Commission may **(…)** decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any specific authorisation.

81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. Apart from the international commitments the third country or international organisation has entered into, the Commission should also take account of participation in a suitable international data protection system established in third countries or a territory or a processing sector. **The Commission should consult with the European Data Protection Board when assessing the level of protection in third countries or international organisations.**

82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation (…) no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements of Articles 42 to 44 are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. **The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.**

83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. **They should relate in particular to compliance with the general principles relating to personal data processing, the availability of data subject's rights and effective legal remedies are available and the principles of data protection by design and by default.**

84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract, including in a contract between the processor and another processor, nor to add other clauses or additional safeguards as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.

85) A corporate group or a group of enterprises engaged in a joint economic activity should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings or group of enterprises, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.

87) These rules should in particular apply to data transfers required and necessary for the protection of (…) reasons of public interest, for example in cases of international data exchange, either spontaneous or on request, between competition authorities, between tax or customs administrations, between financial supervisory authorities, between services competent for social security matters or for public health, or between competent authorities for the prevention, investigation, detection and prosecution of criminal offences, including for the prevention of money laundering and the fight against terrorist financing. A transfer of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's life, if the data subject is incapable of giving consent. **In the absence of an adequacy decision or of appropriate safeguards, Union law or Member State law may, for important reasons of public interest, expressly prohibit the controller or processor to transfer personal data to a third country or an international organisation.**

88) Transfers which cannot be qualified as large scale or frequent, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller or the processor has assessed all the circumstances surrounding the data transfer. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. To assess whether a transfer is large scale or frequent the amount of personal data and number of data subjects should be taken into account and whether the transfer takes place on an occasional or regular basis.

89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred.

90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. (…).

91) When personal data moves across borders outside the Union it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international co-operation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in compliance with the provisions of this Regulation, including those laid down in Chapter V.

107) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities without voting rights. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, **in particular on the level of protection in third countries or international organisations,** and promoting co-operation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.

Article 4

Definitions

For the purposes of this Regulation:

(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;

(21) ‘international organisation’ means an organisation and its subordinate bodies governed by public international law or any other body which is set up by, or on the basis of, an agreement between two or more countries;

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Article 40

General principle for transfers

(…).

Article 41

Transfers with an adequacy decision

1. A transfer of personal data to a recipient or recipients in a third country or an international organisation may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
   (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation (…), data protection rules and security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or by that international organisation, as well as the existence of effective and enforceable data subject rights and effective administrative and judicial redress for data subjects whose personal data are being transferred (…);
   (b) the existence and effective functioning of one or more independent supervisory authorities in the third country, or to which an international organisation is subject, with responsibility for ensuring compliance with the data protection rules **including adequate sanctioning powers** for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, **in particular** in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. **(…).** The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2).

3a. *Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission* **in accordance with the examination procedure referred to in Article 87(2). (…)**

4. (…)

4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC.

5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 and may, where necessary, repeal, amend or suspend such decision without retro-active effect. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2) or, in cases of extreme urgency (…), in accordance with the procedure referred to in Article 87(3). **(…)**

6. A decision pursuant to paragraph 5 is without prejudice to transfers of personal data to the third country, or the territory or (…) processing sector within that third country, or the international organisation in question pursuant to Articles 42 to 44. (…)The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the Decision made pursuant to paragraph 5.

7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country and international organisations in respect of which decisions have been taken pursuant to paragraphs 3 and 5.

8. (…)

Article 42

Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a recipient or recipients in a third country or an international organisation only if the controller or processor has adduced appropriate safeguards *in a legally binding instrument* with respect to the protection of personal data **or where the controller or the processor has obtained prior authorisation for the transfer by the supervisory authority in accordance with paragraph 5.**

2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:
   (a) binding corporate rules **referred to in** Article 43; or
   (b) standard data protection clauses adopted by the Commission (…) in accordance with the examination procedure referred to in Article 87(2); or

(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 and adopted by the Commission pursuant to the examination procedure referred to in Article 87(2); or

(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority pursuant to paragraph 4; or

(e) an approved code of conduct pursuant to Article 38; or

(f) a certification mechanism pursuant to Article 39:

3. A transfer based on *binding corporate rules or standard data protection clauses* as referred to in points (a), (b) or (c) of paragraph 2 shall not require any specific authorisation.

4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 (…), the controller or processor shall obtain prior authorisation of the contractual clauses (…) from the competent supervisory authority (…).

5. Where, notwithstanding the requirement for a legally binding instrument in paragraph 1, appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor **(…)**shall obtain prior authorisation from the competent supervisory authority for any transfer, or category of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such a transfer (…).

5a. If the transfer referred to in paragraph 4 (…)is related to processing activities which concern data subjects in several Member States, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

5b. *Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed by that supervisory authority.*

Article 43

Transfers by way of binding corporate rules

1. The competent supervisory authority shall *approve binding corporate rules* in accordance with the consistency mechanism set out in Article 58 (…) provided that they:
   (a) are legally binding and apply to, and are enforced by, every member concerned of the group of undertakings or group of enterprises engaged in a joint economic activity;
   (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data;
   (c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall **contain a description of** at least the following elements:
   (a) the structure and contact details of the group concerned and of each of its members;
   (b) the data transfers or categories of transfers, including the types of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
   (c) their legally binding nature, both internally and externally;
   (d) application of the general data protection principles, in particular purpose limitation, including the purposes which govern further processing, data quality, legal basis for the processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies (…) not bound by the binding corporate rules;

(e) the rights of data subjects in regard to the processing of their personal data and the means to exercise these rights, including the right not to be subject to (…) profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, on proving that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Articles 14 and 14a;

(h) the tasks of any data protection officer designated in accordance with Article 35, including monitoring (…) compliance with the binding corporate rules within the group, as well as monitoring the training and complaint handling;

(hh) the complaint procedures;

(i) the mechanisms within the group (…) for ensuring the verification of compliance with the binding corporate rules;

(j) the mechanisms for reporting and recording changes to the rules and reporting these changes to the supervisory authority;

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group (…), in particular by making available to the supervisory authority the results of (…) verifications of the measures referred to in point (i) of this paragraph.

[3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.]

4. The Commission may specify the format and procedures for the exchange of information (…) between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Article 44

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 41, of appropriate safeguards pursuant to Article 42, **or of binding corporate rules pursuant to Article 43** a transfer or a category of transfers of personal data to **a recipient or recipients in** a third country or an international organisation may take place only on condition that:
   (a) the data subject has consented to the proposed transfer, after having been informed **that** such transfers **may pose** *risks* due to the absence of an adequacy decision and appropriate safeguards; or
   (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or
   (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) the transfer is necessary for reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

(h) the transfer *which* is not large scale or *frequent*, is necessary for the purposes of legitimate interests pursued by the controller or the processor **which are not overridden by the interests or rights and freedoms of the data subject** and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and, *where necessary*, based on this assessment adduced suitable safeguards with respect to the protection of personal data.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. (…)

4. Points (a), (b), (c) **and (h)** of paragraph 1shall not apply to activities carried out by public authorities in the exercise of their public powers.

5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the national law of the Member State to which the controller is subject. **Union law or Member State law may, for important reasons of public interest, expressly prohibit the controller or processor to transfer personal data to a third country or an international organisation.**

6. The controller or processor shall document the assessment as well as the suitable safeguards (…) referred to in point (h) of paragraph 1 in the records referred to in Article 28 (…).

6a. (…)

7. (…).

Article 45

International co-operation for the protection of personal data

1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:
   (a) develop international co-operation mechanisms to facilitate the *effective* enforcement of legislation for the protection of personal data;
   (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through (…) complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
   (c) engage relevant stakeholders in discussion and activities aimed at promoting international co-operation in the enforcement of legislation for the protection of personal data;
   (d) promote the exchange and documentation of personal data protection legislation and practice.

2. For the purposes of paragraph 1, the Commission **and supervisory authorities** shall take appropriate steps to advance the relationship with third countries and international organisations, including their supervisory authorities, in particular where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).

CHAPTER VII
SECTION 3
EUROPEAN DATA PROTECTION BOARD

Article 66

***Tasks of the European Data Protection Board**r*

(referred only the provisions that relate to international transfers)

1. The European Data Protection Board shall promote the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:

   (cb) give the Commission an opinion on the level of protection in third countries or international organisations, in particular in the cases referred to **in Article 41**;

   (f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;

   (g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide;

2. Where the Commission requests advice from the European Data Protection Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public.

4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

Article 67

Reports

1. (…).

2 The European Data Protection Board *shall draw up an annual report regarding the protection of natural persons with regard to the processing of personal data in the Union and*, where relevant, *in third countries* and international organisations. The report shall be made public and be transmitted to the European Parliament, the Council and the Commission.

3. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).

_____

PSEUDONYMISIERUNG

23) Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Um festzustellen, ob eine Person bestimmbar ist, sind alle Mittel zu berücksichtigen, die von dem für die Verarbeitung Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen aller Voraussicht nach genutzt werden, um die Person direkt oder indirekt zu identifizieren. Bei Prüfung der Frage, ob Mittel nach allgemeinem Ermessen aller Voraussicht nach zur Identifizierung der Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei sowohl die zum Zeitpunkt der Verarbeitung verfügbare Technologie als auch die technologische Entwicklung zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Daten gelten, d.h. für Daten, die sich nicht auf eine bestimmte oder bestimmbare natürliche Person beziehen oder Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische und für Forschungszwecke. Die Grundsätze des Datenschutzes sollten nicht für Verstorbene gelten, es sei denn, die Informationen über Verstorbene beziehen sich auf eine bestimmte oder bestimmbare natürliche Person.

Pseudonymisierte Daten, die allein schon durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine bestimmbare natürliche Person betrachtet werden, wobei alle Mittel, die von dem für die Verarbeitung Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen aller Voraussicht nach zur Identifizierung der Person genutzt werden, zu berücksichtigen sind. Die Grundsätze des Datenschutzes sollten auch gelten, wenn eine Person durch Heranziehung zusätzlicher Informationen bestimmt werden kann, wobei alle Mittel, die von dem für die Verarbeitung Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen aller Voraussicht nach zur Identifizierung der Person genutzt werden, zu berücksichtigen sind.

(39) Die Verarbeitung von Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams – CERT, beziehungsweise Computer Security Incident Response Teams – CSIRT), Betreiber von elektronischen Kommunikationsnetzen und diensten sowie durch Anbieter von Sicherheitstechnologien und diensten stellt in dem Maße ein berechtigtes Interesse des jeweiligen für die Verarbeitung Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen, die Verbreitung schädlicher Programmcodes, die Abwehr von Angriffen in Form der gezielten Überlastung von Servern ("Denial of access"-Angriffe) sowie Schädigungen von Computer- und elektronischen Kommunikationssystemen zu verhindern. **Die Verarbeitung personenbezogener Daten in dem für die Verhinderung von Betrug unbedingt erforderlichen Umfang ist ebenfalls ein berechtigtes Interesse des jeweiligen für die Verarbeitung Verantwortlichen. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als einem rechtmäßigen Interesse dienende Verarbeitung betrachtet werden.**

45) Kann der für die Verarbeitung Verantwortliche anhand der von ihm verarbeiteten Daten eine natürliche Person nicht bestimmen **(...)**, sollte er nicht verpflichtet sein, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu bestimmen. (…). Allerdings sollte er sich nicht weigern, **zusätzliche** Informationen, die von der betroffenen Person beigebracht werden, um ihre Rechte geltend zu machen, entgegenzunehmen.

Artikel 4

Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck

[...]

(3b) "Pseudonymisierung" die Verarbeitung **personenbezogener Daten in einer Weise, dass sie 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 die Nichtzuordnung gewährleisten.**

Artikel 14 a

Informationspflicht, wenn die Daten nicht bei der betroffenen Person erhoben wurden

(4) Die Absätze 1 bis 3 finden keine Anwendung, wenn und soweit

b) die Erteilung dieser Informationen **(...)** sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde oder die Wahrscheinlichkeit besteht, dass sie die Erreichung der Zwecke der Verarbeitung unmöglich macht oder ihr ernsthaft entgegensteht; in diesen Fällen ergreift der für die Verarbeitung Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, oder

Artikel 23

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

(1) Der für die Verarbeitung Verantwortliche trifft unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten sowie der Risiken, die aufgrund der Art, des Umfangs und des Zwecks der Verarbeitung für die Rechte und Freiheiten von Personen bestehen, der Verarbeitungstätigkeit und ihren Zielen angemessene technische und organisatorische Maßnahmen, einschließlich der **Pseudonymisierung der personenbezogenen** Daten, durch die sichergestellt wird, dass die Verarbeitung den Anforderungen dieser Verordnung genügt und dass die Rechte **und Freiheiten** der betroffenen Person (...) gewahrt werden.

Artikel 30

Sicherheit der Verarbeitung

(1) Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten sowie der Art, der Umstände, des Umfangs und des Zwecks der Verarbeitung und der Risiken für die Rechte und Freiheiten der betroffenen Personen technische und organisatorische Maßnahmen, einschließlich der **Pseudonymisierung der personenbezogenen** Daten, die geeignet sind, ein diesen Risiken angemessenes Schutzniveau zu gewährleisten.

Artikel 32

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(3) Die Benachrichtigung der betroffenen Person (...) gemäß Absatz 1 ist nicht erforderlich, wenn

a. der für die Verarbeitung Verantwortliche (...) geeignete technische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die betreffenden Daten für alle Personen, die nicht zum Zugriff auf die Daten befugt sind, unverständlich gemacht werden, etwa durch Verschlüsselung **(...)**; oder

Artikel 38

Verhaltensregeln

(1a) Verbände und andere Gremien, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern vertreten, können Verhaltensregeln ausarbeiten bzw. ändern oder ergänzen, um die Anwendung von Bestimmungen dieser Richtlinie beispielsweise in Bezug auf folgende Aspekte zu präzisieren:

bb) **Pseudonymisierung personenbezogener** Daten;

_____

ÜBERTRAGBARKEIT PERSONENBEZOGENER DATEN

(51) Eine natürliche Person sollte ein Auskunftsrecht hinsichtlich der Daten, die bei ihr erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich von der Rechtmäßigkeit der Verarbeitung überzeugen zu können. Dies schließt das Recht natürlicher Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten. Jede betroffene Person sollte daher ein Anrecht darauf haben zu wissen und zu erfahren, zu welchen Zwecken die Daten verarbeitet werden und, wenn möglich, wie lange sie gespeichert werden, wer die Empfänger der Daten sind, nach welcher Logik die Daten verarbeitet werden und welche Folgen eine solche Verarbeitung haben kann, zumindest in Fällen, in denen die Verarbeitung auf Profiling basiert. Dabei dürfen die Grundrechte und Grundfreiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigem Eigentums und insbesondere das Urheberrecht an Software, nicht angetastet werden. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird. Verarbeitet der für die Verarbeitung Verantwortliche eine große Menge von Informationen über die betroffene Person, so kann er verlangen, dass diese präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt. **Damit die betroffene Person ihr Recht auf Auskunft über ihre eigenen Daten besser ausüben kann, sollte sie im Falle einer elektronischen Verarbeitung ihrer personenbezogenen Daten in einem strukturierten gängigen Format Anspruch darauf haben, eine Kopie der sie betreffenden Daten ebenfalls in einem gängigen elektronischen Format zu erhalten.**

(55) Damit die betroffene Person eine bessere Kontrolle über ihre eigenen Daten hat **(...)**, sollte sie im Falle einer elektronischen Verarbeitung ihrer personenbezogenen Daten auch das Recht haben, die von ihr zur Verfügung gestellten personenbezogenen Daten **in einem gängigen Format** aus einem automatisierten Verarbeitungssystem zurückzuziehen und auf ein anderes **automatisiertes Verarbeitungssystem** zu übertragen.

Dies sollte dann gelten, wenn die betroffene Person die personenbezogenen Daten dem automatisierten Verarbeitungssystem mit ihrer ausdrücklichen Einwilligung oder im Zuge der Erfüllung eines Vertrags zur Verfügung gestellt hat. **Es sollte nicht gelten, wenn die Verarbeitung auf einer anderen Rechtsgrundlage** als ihrer ausdrücklichen Einwilligung oder eines Vertrags **erfolgt**. **Dieses Recht sollte naturgemäß nicht gegen für die Verarbeitung Verantwortliche, die Daten in Erfüllung ihrer öffentlichen Aufgaben verarbeiten, ausgeübt werden. Es sollte daher insbesondere nicht gelten, wenn die Verarbeitung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt, oder für die Wahrnehmung einer ihm übertragenen Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, erforderlich ist.**

Bezieht sich eine bestimmte Sammlung personenbezogener Daten auf mehrere betroffene Personen, so sollte das Recht, die Daten zurückzuziehen und auf ein anderes automatisiertes Verarbeitungssystem zu übertragen, **die Anforderungen in Bezug auf die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten, die sich auf eine andere betroffene Person beziehen, gemäß dieser Verordnung nicht berühren**. **Dieses Recht sollte zudem das Recht der betroffenen Person auf Löschung ihrer personenbezogenen Daten und die Beschränkungen dieses Rechts gemäß dieser Verordnung nicht berühren und insbesondere nicht** bedeuten, dass die Daten, die sich auf die betroffene Person beziehen und von ihr zur Erfüllung eines Vertrags zur Verfügung gestellt worden sind, gelöscht werden, sofern und solange diese Daten für die Erfüllung des Vertrags notwendig sind. **(…)**

Artikel 18

Recht auf Datenübertragbarkeit

(1) (…)

(2) Hat die betroffene Person die personenbezogenen Daten zur Verfügung gestellt und erfolgt die Verarbeitung – auf Basis einer Einwilligung oder eines Vertrags – mittels eines automatisierten Verarbeitungssystems[, das durch einen Dienst der Informationsgesellschaft betrieben wird], so hat die betroffene Person **unbeschadet des Artikels 17** das Recht, diese Daten (...) in **einem gängigen Format** zurückzuziehen **und sie** auf ein anderes automatisiertes Verarbeitungssystem zu übertragen, ohne dabei von dem für die Verarbeitung Verantwortlichen, dem die personenbezogenen Daten entzogen werden, behindert zu werden.

(2a) Das Recht nach Absatz 2 berührt nicht die Rechte des geistigen Eigentums **in Bezug auf die Verarbeitung der Daten in automatisierten Verarbeitungssystemen**.

[2b. Das Recht nach Absatz 2 gilt nicht für die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstaben c, d, e und f.]

[(3) Die Kommission kann (...) die technischen Standards, Modalitäten und Verfahren für die Überführung der personenbezogenen Daten gemäß Absatz 2 festlegen. Die betreffenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen].

(4) (…)

PFLICHTEN DER FÜR DIE VERARBEITUNG VERANTWORTLICHEN UND DER AUFTRAGSVERARBEITER

(63a) Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter im Namen des für die Verarbeitung Verantwortlichen vorzunehmende Verarbeitung eingehalten werden, sollte ein für die Verarbeitung Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, nur mit Auftragsverarbeitern arbeiten, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen – hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, **die** den Anforderungen dieser Verordnung zu genügen. Als Nachweis für das Vorliegen solcher hinreichenden Garantien gilt die Tatsache, dass der Auftragsverarbeiter einen Verhaltenskodex oder ein Zertifizierungsverfahren einhält. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf Grundlage eines Vertrags oder eines anderen Rechtsakts erfolgen, der den Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen bindet und in dem Inhalt und Geltungsdauer des Vertrags, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt sind, wobei die besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung und die Risiken für die Rechte und Freiheiten der betroffenen Person zu berücksichtigen sind. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter können entscheiden, ob sie einen individuellen Vertrag oder Standardvertragsklauseln verwenden, die entweder von der Kommission erlassen oder aber nach dem Kohärenzverfahren von einer Aufsichtsbehörde erlassen und von der Kommission genehmigt wurden oder Bestandteil einer im Rahmen des Zertifizierungsverfahrens erteilten Zertifizierung sind. Jeder Auftragsverarbeiter, der personenbezogene Daten auf eine andere als die ihm von dem für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet, sollte für diese Verarbeitung als für die Verarbeitung Verantwortlicher gelten. Nach Beendigung der Verarbeitung im Namen des für die Verarbeitung Verantwortlichen sollte der Auftragsverarbeiter die personenbezogenen Daten zurückgeben oder löschen, sofern nicht nach dem Unionsrecht oder dem Recht des Mitgliedstaats, dem er unterliegt, eine Verpflichtung zur Speicherung der Daten besteht; dabei sollte er geeignete Maßnahmen treffen, um die Sicherheit und Vertraulichkeit der personenbezogenen Daten zu gewährleisten, und diese Daten nicht mehr aktiv weiterverarbeiten.

Artikel 26

Auftragsverarbeiter

(1) Der für die Verarbeitung Verantwortliche (...) arbeitet nur mit Auftragsverarbeitern, die hinreichende Garantien dafür bieten, dass die betreffenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt (...).

(1a) Als Nachweis für das Vorliegen hinreichender Garantien im Sinne der Absätze 1 und 2a gilt die Tatsache, dass **der Auftragsverarbeiter** einen Verhaltenskodex gemäß Artikel 38 oder ein Zertifizierungsverfahren gemäß Artikel 39 einhält.

(2) Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsakt, der den Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen bindet und in dem Inhalt und Geltungsdauer des Vertrags, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt sind und insbesondere vorgesehen ist, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf Weisung des für die Verarbeitung Verantwortlichen (...) verarbeitet, sofern er nicht nach dem Unionsrecht oder dem Recht des Mitgliedstaats, dem er unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dies dem für die Verarbeitung Verantwortlichen mit, sofern das Unionsrecht oder das Recht des Mitgliedstaats, dem er unterliegt, eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

b) (…)

c) alle gemäß Artikel 30 erforderlichen Maßnahmen ergreift;

d) die Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters (...) festlegt, etwa dass der für die Verarbeitung Verantwortliche ihr zuvor ausdrücklich zugestimmt haben muss;

e) soweit es angesichts der Art der Verarbeitung (...) möglich ist, den für die Verarbeitung Verantwortlichen dabei unterstützt, Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) festlegt, wie der für die Verarbeitung Verantwortliche bei der Einhaltung der in den Artikeln 30 bis 34 genannten Pflichten zu unterstützen ist;

g) die personenbezogenen Daten nach Beendigung der Verarbeitung, die in dem Vertrag oder dem sonstigen Rechtsakt angegeben ist, wahlweise zurückgibt oder löscht, sofern nicht nach dem Unionsrecht oder dem Recht des Mitgliedstaats, dem er unterliegt, eine Verpflichtung zur Speicherung der Daten besteht; dabei trifft er geeignete Maßnahmen, um die Sicherheit und Vertraulichkeit der personenbezogenen Daten zu gewährleisten;

h) dem für die Verarbeitung Verantwortlichen (...) alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt.

(2a) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstägigkeiten im Namen des für die Verarbeitung Verantwortlichen auszuführen, so muss dieser weitere Auftragsverarbeiter hinreichende Garantien dafür bieten, dass die betreffenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt.

(2aa) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstägigkeiten im Namen des für die Verarbeitung Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter in einem Vertrag oder einem anderen Rechtsakt dieselben Pflichten auferlegt, die in dem Vertrag oder anderen Rechtsakt zwischen dem für Verarbeitung Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 2 festgelegt sind.

(2ab) Unbeschadet eines individuellen Vertrags zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder der andere Rechtsakt im Sinne der Absätze 2 und 2aa ganz oder teilweise auf den in den Absätzen 2b und 2c genannten Standardvertragsklauseln oder aber auf Standardvertragsklauseln beruhen, die Bestandteil einer dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 39 und 39a erteilten Zertifizierung sind.

(2b) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in Absatz 2 genannten Fragen festlegen.

(2c) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 57 Standardvertragsklauseln zur Regelung der in Absatz 2 genannten Fragen festlegen.

(3) Der Vertrag oder der andere Rechstakt im Sinne der Absätze 2 und 2a ist schriftlich oder in einem elektronischen oder einem anderen ohne technische Vermittlung nicht lesbaren Format, das in ein lesbares Format umgewandelt werden kann, abzufassen.

(4) (…)

(5) (…)

_____