Microsoft
Corporate Affairs Europe | Tel +32 (0) 2 704 39 10
Avenue de Nerviens 85 | B-1040 Brussels

Für weitere Informationen kontaktieren Sie bitte Jean Gonié, Director of Privacy EMEA Policy
oder Tanja Böhm, Manager Government Affairs, tanja.boehm@microsoft.com
oder Jörg-Alexander Albrecht, Manager Government Affairs, a-joalb@microsoft.com

Microsoft präsentiert Positionen und Vorschläge zum vorliegenden Entwurf für die *Datenschutz-Grundverordnung*

Microsoft begrüßt den Entwurf für die Datenschutz-Grundverordnung. Als Unternehmen schützen wir die Privatsphäre der Anwender. Wir legen Wert darauf, unsere Datenschutzbestimmungen für unsere Kunden transparent zu gestalten, und wir arbeiten mit Nachdruck an der Entwicklung von Innovationen, die unseren Kunden beim Umgang mit ihren personenbezogenen Daten ein hohes Maß an Kontrolle und Mitsprache gewähren. Unsere Bemühungen spiegeln sich in unseren Produkten und Services wider, beispielsweise in unserer Entscheidung, im Internet Explorer 10 das "Do not Track" Signal zu aktivieren, sowie in unserem Office 365 Trust Center, über das die Nutzer unserer Cloud Services Zugang zu detaillierten Informationen zu unseren Datenschutzbestimmungen und -praktiken erhalten.

Wir sind davon überzeugt, dass sowohl Industrie als auch Verbraucher von klaren und harmonisierten datenschutzrechtlichen Bestimmungen profitieren können. Aber wir sind uns auch bewusst, dass insbesondere Online-Unternehmen ein gewisses Maß an Flexibilität benötigen, um Innovationen und neue Lösungen für den Datenschutz entwickeln zu können. Mit den von uns vorgeschlagenen Ergänzungen zielen wir auf dieses Gleichgewicht ab: Unternehmen sollen strenge datenschutzrechtliche Bestimmungen einhalten und ein hohes Maß an Transparenz und Nachvollziehbarkeit bieten, und gleichzeitig sollen die zahlreichen Vorteile austariert werden, die durch aktuelle Technologien ermöglicht werden. Die von uns erarbeiteten Vorschläge betreffen insbesondere die folgenden Punkte:

1/ Regeln zur Stärkung von sicheren Datentransfers in der Cloud (S. 5). *Die erste von uns vorgeschlagene Ergänzung fördert bewährte positive Praktiken, indem Organisationen dafür belohnt werden, dass sie die relevanten Schutzbestimmungen auch auf die von ihnen außerhalb der EU übertragenen Daten anwenden, einschließlich auf Datentransfers in der Cloud. Darüber hinaus schlagen wir eine Ergänzung vor, durch welche die soliden EU-Schutzbestimmungen für Datentransfers an Subbeauftragte zur Datenverarbeitung ausgeweitet und standardisiert werden, wie sie innerhalb der Cloud kontinuierlich an Bedeutung gewinnen.*

2/ Klarere Regelungen für die für die Datenverarbeitung Verantwortlichen und für Auftragsdatenverarbeiter (S. 11). *Nach Maßgabe der vorgeschlagenen Regulierungsvorschriften sind die für die Datenverarbeitung Verantwortlichen und Auftragsverarbeiter unterschiedlichen Verpflichtungen unterworfen. Wir schlagen ein klares Testverfahren vor, mit dem Unternehmen* ihren Status ermitteln (d.h. für die Datenverarbeitung Verantwortlicher oder Auftragsverarbeiter) und damit verbindlich feststellen können, welche Aufsichtsbehörde für sie zuständig ist.

3/ Effektivere Benachrichtigungen bei Verletzungen (S. 16). *Effektive Benachrichtigungen bei Verfehlungen stärken die Datensicherheit und die Transparenz innerhalb der gesamten Branche. Mit der von uns vorgeschlagenen Ergänzung würden Regeln für die Benachrichtigung bei Verfehlungen gewährleistet, die sicherstellen, dass Datensubjekte Mitteilungen im Zusammenhang mit ihren Datenschutzinteressen aufmerksam wahrnehmen.*

4/ Spürbare, aber angemessene Strafen (S. 18)*. Die Verhängung von Bußgeldern ist ein essenzieller Bestandteil des neuen regulatorischen Rahmens. Der vorgesehene einheitliche Ansatz würde jedoch vorsätzliche und versehentliche Verstöße ohne jede Unterscheidung behandeln. Wir sehen hierin eine Verletzung der Verhältnismäßigkeit. Die von uns vorgeschlagene Regelung gäbe Datenschutzbehörden die Möglichkeit, empfindliche, aber faire Bußgelder zu verhängen.*

5/ Delegierte Rechtsakte auf ein Minimum reduzieren (S. 22)*. Die bloße Anzahl der delegierten Rechtsakte dürfte zu erheblicher Unsicherheit bei Unternehmen und Verbrauchern führen. Durch die von uns vorgeschlagenen Anpassungen würde die Zahl der delegierten Rechtsakte reduziert.*

***

Microsoft begrüßt die Bemühungen zur Stärkung und Harmonisierung der EU-Datenschutzbestimmungen. Das Vertrauen unserer Kunden ist unser wichtigstes Kapital, und bei der Entwicklung unserer Technologien spielt der Schutz personenbezogener Daten eine konstante Rolle. In einer Zeit, in der die ständige Verbindung mit dem Internet, Online-Business und soziale Netzwerke allgegenwärtig sind und Informationen auf der ganzen Welt auf den unterschiedlichsten Computern und Geräten verschickt und gespeichert werden, ist unsere Priorität der Schutz personenbezogener Daten.

Wie wir aus eigener Erfahrung wissen, liegt die Herausforderung für uns im Schutz der personenbezogenen Daten der europäischen Verbraucher bei gleichzeitiger Förderung innovativer Entwicklungen. Um dieses Ziel zu erreichen, müssen wir einen schwierigen Balanceakt vollführen. Einerseits müssen Daten verarbeitende Unternehmen ihre Praktiken bei der Datenverarbeitung nachvollziehbar und transparent gestalten und ein hohes Maß an Datenschutz gewährleisten. Gleichzeitig sollte der regulatorische Rahmen der EU jedoch nicht vorschreiben, wie genau Datenschutzbestimmungen umzusetzen sind und davon absehen, neue Belastungen für die für die Datenverarbeitung Verantwortlichen sowie für Auftragsdatenverarbeiter zu schaffen, die letztendlich keinen positiven Beitrag zum Schutz personenbezogener Daten leisten.

Stattdessen sollte Unternehmen die Möglichkeit gegeben werden, flexible und den jeweiligen Umständen angemessenen Datenschutzlösungen zu entwickeln. Durch starke Anreize sollte die innovative Entwicklung der bestmöglichen Lösungen zum Schutz personenbezogener Daten gefördert werden. Im Gegenzug sollten Unternehmen, welche die ihnen anvertrauten Daten nicht angemessen sichern und schützen, durch empfindliche Strafen gemaßregelt werden.

Die von uns vorgeschlagenen Anpassungen stellen in diesem Zusammenhang einen wichtigen Schritt nach vorne dar. Beispielsweise enthält unser Vorschlag Regelungen, denen zufolge Unternehmen neue Technologien unter kontinuierlicher Berücksichtigung datenschutzrechtlicher Anforderungen entwickeln, ihre interne Datenverarbeitung transparent gestalten und Verantwortung für ihren Umgang mit personenbezogenen Daten übernehmen. Die von uns vorgeschlagenen Anpassungen korrigieren zudem inkonsistente Bestimmungen und Interpretationen in den 27 EU-Mitgliedsstaaten, wie beispielsweise den Ansatz einer zentralen Anlaufstelle für den Datenschutz („One Stop Shop“-Ansatz).

Andere der vorgeschlagenen Elemente bedürfen dagegen noch einer Überarbeitung, um sicherzustellen, dass sie sowohl soliden Schutz bieten als auch praxistauglich sind. Aus diesem Grund sind wir überzeugt, dass gewisse Ergänzungen durchaus angemessen sind, insbesondere im Zusammenhang mit den folgenden Punkten:

1. **Internationale Datentransfers.** Die Grundverordnung führt wichtige Mechanismen ein, die den sicheren Fluss personenbezogener Daten erleichtern, einschließlich in der Cloud. Zu diesen Mechanismen zählen sogenannte Standard-Datenschutzklauseln (*Standard Contractual Clauses*, SCCs). Standard-Datenschutzklauseln verpflichten Unternehmen zur Einhaltung grundlegender Schutzmaßnahmen bei der Datenübertragung und werden mittlerweile standardmäßig bei der Übertragung von Daten außerhalb der EU angewandt. Microsoft setzt sich mit Nachdruck für derartige Standard-Datenschutzklauseln ein und bietet diese seinen Unternehmenskunden für Clouddienste an. Wir vertreten jedoch auch die Position, **dass Datenverarbeiter in der Cloud und andere Teilnehmer dazu ermutigt werden sollten, in bestimmten Situationen über die in den Standard-Datenschutzklauseln vorgeschriebenen grundlegenden Sicherheitsvorschriften *noch hinauszugehen***.

   Durch die von uns vorgeschlagenen Ergänzungen würde der hierfür erforderliche Mechanismus geschaffen. Die von uns vorgeschlagenen Ergänzungen sehen insbesondere eine Anpassung von Artikel 42 vor, um Unternehmen einen *Anreiz* (etwa in Form eines EU-Güte- oder -Datenschutzsiegels) zu bieten, zusätzliche Sicherungsmechanismen bei der Datenübertragung umzusetzen. Darüber hinaus schlagen wir eine Anpassung von Artikel 39 (betreffend Zertifizierungen) vor, wonach sämtliche Mechanismen für Siegel oder Zertifikate freiwillig, finanzierbar, technologieneutral, transparent und global einsetzbar sein müssen. Auf diese Weise kann sichergestellt werden, dass Zertifizierungen die größtmögliche Verbreitung und Unterstützung bei den für die Datenverarbeitung Verantwortlichen sowie bei Auftragsverarbeitern finden.

   Des Weiteren umfassen die von uns erarbeiteten Vorschläge eine Ergänzung zur Ausweitung der standardmäßig bei Subbeauftragten eingesetzten Standard-Datenschutzklauseln gemäß den Empfehlungen auf Seite 74 und Seite 80 der vom European Parliament Policy Department für den IMCO-Ausschuss für Binnenmarkt und Verbraucherschutz erstellten Studie „Reforming the Data Protection Package"[1] (die „Parliament Study"). Heutzutage sind die Anbieter von Cloud-Diensten oftmals auf Subbeauftragte zur Datenverarbeitung angewiesen. Die Ausweitung der Standard-Datenschutzklauseln auf Subbeauftragte gewährt den in der EU ansässigen Anbietern von Cloud-Diensten mehr Flexibilität bei der Auswahl ihrer Subunternehmer und Verbrauchern die Gewissheit sicherer Datenübertragungen. Dieser Ansatz entspricht den in der Parliament Study abgegebenen Empfehlungen. Er entspricht auch der Empfehlung der Stellungnahme der Arbeitsgruppe zu Artikel 29 vom Mai 2012 im Zusammenhang mit Cloud-Diensten, in der die Arbeitsgruppe vorschlägt, die in den Standard-Datenschutzklauseln vorgesehen Verpflichtungen für Auftragsverarbeiter schriftlich auf Subbeauftragte auszuweiten.

2. **Für die Datenverarbeitung Verantwortliche und Auftragsverarbeiter**. Im Einklang mit den bestehenden EU-Vorschriften sieht der aktuelle Vorschlag auch weiterhin eine Aufteilung der Verantwortlichkeiten zwischen den „für die Datenverarbeitung Verantwortlichen" und „Auftragsverarbeitern" vor. Da die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter unterschiedlichen Verpflichtungen unterliegen, ist es von zentraler Bedeutung, dass Unternehmen nachvollziehen können, wann sie in welcher Rolle agieren. **Die von uns**

[1] „Reforming the Data Protection Package" Studie, S. 74, 80 - Directorate-General for Internal Policies, Policy Department, Economic and Scientific Policy, Internal Market and Consumer Protection, verfügbar unter http://www.europarl.europa.eu/document/activities/cont/201209/20120928ATT52488/20120928ATT52488EN.pdf

erarbeiteten Vorschläge bewirken eine klarere Abgrenzung zwischen den für die Datenverarbeitung Verantwortlichen und Auftragsverarbeitern: Entscheidet ein Unternehmen darüber, zu welchem Zweck personenbezogene Daten verarbeitet werden, so agiert es als ein für die Datenverarbeitung Verantwortlicher. Entscheidet ein Unternehmen lediglich über die Art der Verarbeitung personenbezogener Daten (d.h. über Mittel und Konditionen der Verarbeitung), so agiert es als Auftragsverarbeiter. Dieser Ansatz entspricht einer in der Parliament Study[2]abgegebenen Empfehlung.

Die von uns vorgeschlagenen Ergänzungen würden es Unternehmen darüber hinaus **erleichtern, ihre zentrale Anlaufstelle für den Datenschutz zu bestimmen**. Derzeit unterliegen europaweit agierende Unternehmen zahlreichen unterschiedlichen und voneinander abweichenden nationalen Datenschutzbestimmungen. Um dieses Umstand zu begegnen, sieht die Datenschutz-Grundverordnung vor, dass für Unternehmen lediglich die Bestimmungen des Landes gelten, in dem die jeweilige Hauptniederlassung liegt („*One Stop Shop*"-Ansatz). Gleichzeitig sehen die Bestimmungen jedoch *unterschiedliche* Tests für die für die Datenverarbeitung Verantwortlichen und für Auftragsverarbeiter bei der Bestimmung ihres Hauptsitzlandes vor. Ähnlich wie bei der Definition der Begriffe des „für die Datenverarbeitung Verantwortlichen" und des „Auftragsverarbeiters" geht der Ansatz bei der „Hauptniederlassung" nicht darauf ein, wie viele Organisationen jeweils operativ sind. In der Praxis agieren zahlreiche der für die Datenverarbeitung Verantwortlichen auch als Auftragsverarbeiter. Die Einführung *unterschiedlicher* Tests zur Bestimmung der Hauptniederlassung der Verantwortlichen für die Datenverarbeitung bzw. der Auftragsverarbeiter hätte zur Folge, dass diejenigen der für die Datenverarbeitung Verantwortlichen, die auch als Auftragsverarbeiter agieren, auf nationaler Ebene auch weiterhin unterschiedlichen Behörden unterworfen wären. Der von uns erarbeitete Vorschlag sieht vor, dass die für die Datenverarbeitung Verantwortlichen den *gleichen* Tests wie Auftragsverarbeiter unterworfen werden, wenn sie beide Funktionen übernehmen.

3. **Verletzungen des Datenschutzes:** Die verbindliche Meldung schwerwiegender Verstöße gegen datenschutzrechtliche Bestimmungen durch die für die Datenverarbeitung Verantwortlichen würde höhere Standards bei der Datensicherheit in der gesamten Branche fördern. Die entsprechenden Vorschriften zur Meldung von Verstößen müssten jedoch in der Praxis anwendbar sein. Der vorliegende Entwurf hätte zur Folge, dass die für die Datenverarbeitung Verantwortlichen auch *nicht schwerwiegende* Verstöße melden müssten. Dieser Vorschlag würde eine Überlastung der Datenschutzbehörden und Datensubjekte mit Meldungen zu Verstößen von geringer Tragweite bewirken, sodass Datensubjekte derartige Verstoßmitteilungen letztlich wohlmöglich vollständig ignorieren könnten. So ergibt es beispielsweise keinen Sinn, zwei Fälle als gleichwertig zu behandeln, wenn in einem Fall das Konto eines Computerspielers gehackt wird und der Eindringling Zugang auf die Spielstände des Opfers erhält, während im zweiten Fall die elektronisch gespeicherte Krankheitsgeschichte eines Patienten Gegenstand der Verletzung ist. Die von uns erarbeiteten Vorschläge sollen gewährleisten, dass eine Mitteilung nur dann verbindlich wird, wenn ein erhebliches Schadensrisiko für das Datensubjekt besteht.

4. **Bußgelder / Sanktionen:** Datenschutzrechtliche Verpflichtungen sind nur in dem Umfang wirksam, in dem sie durchgesetzt werden. Vor diesem Hintergrund sieht die Grundverordnung empfindliche Sanktionen bei Verstößen vor. Der Entwurf sieht jedoch einheitliche Strafen vor und könnte dahin

[2] Siehe oben, S. 31, 41.

gehend interpretiert werden, dass vorsätzliche Regelverstöße gleichermaßen geahndet werden wie unbeabsichtigte Verletzungen der Vorschriften. Dies könnte zur Folge haben, dass ein Unternehmen, das unbeabsichtigterweise ein falsches elektronisches Format verwendet, um einem Kunden Zugang zu seinen Daten zu gewähren, die gleichen Sanktionen zu erwarten hat wie ein Unternehmen, das vorsätzlich und wiederholt personenbezogene Daten sammelt und auswertet, ohne die betreffenden Personen hiervon in Kenntnis zu setzen. Um die Verhältnismäßigkeit zu wahren und effektiv zu wirken, müssten in der Grundverordnung empfindlichere Sanktionen für besonders schwere Fälle vorgesehen sein.

5. **Delegierte Rechtsakte:** Die Grundverordnung sieht 26 Fälle vor, in denen die Kommission zum Erlaß delegierter Rechtsakte bemächtigt werden soll. Diese hohe Anzahl der Rechtsakte sollte deutlich reduziert werden. So behandeln beispielsweise zahlreiche Bestimmungen essenzielle gesetzliche Fragen. Derartige essenzielle Rechtsfragen sollten in der Grundverordnung selbst behandelt werden und nicht der Entscheidung durch die Kommission als sekundäre Instanz überlassen sein. In anderen delegierten Rechtsakten wird der Kommission die Kompetenz zur Einführung technischer Formate, Standards und Lösungen übertragen -- wodurch Innovationen durch Unternehmen durch regulatorische Eingriffe zunichte gemacht werden könnten. Der von uns erarbeitete Vorschlag sieht die Löschung derjenigen Bestimmungen vor, die als essenzielle Fragen in der eigentlichen Grundverordnung behandelt und/oder besser auf dem Wege innovativer Entwicklungen gelöst werden sollten. Und schließlich sehen die delegierten Rechtsakte keinen klaren Zeitplan für eine Umsetzung vor (vgl. Arbeitsgruppe zu Artikel 29 und EU-Datenschutzbeauftragter). Die von uns vorgeschlagenen Ergänzungen enthalten eine Frist für die Umsetzung delegierter Rechtsakte.

Internationale Datentransfers/Cloud

Ergänzung
Vorschlag für eine Verordnung
Erwägung 84

Textvorschlag der Kommission	*Ergänzung*
(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 nor to add other clauses 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.	(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 nor to add other clauses 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. ***In some scenarios, it may be appropriate to encourage controllers and processors to provide even more robust safeguards via additional contractual commitments that supplement standard data protection clauses.***

Ergänzung
Vorschlag für eine Verordnung
Artikel 42 - Abschnitt 2e (neu)

Textvorschlag der Kommission	*Ergänzung*
2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: …	2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: … ***(e) contractual clauses between the controller or processor and the recipient of the data that supplement standard data protection clauses as referred to in points (b) and (c) of paragraph 2 of this Article, and are authorised by the competent supervisory***

authority in accordance with paragraph 4.

Ergänzung
Vorschlag für eine Verordnung
Artikel 42 – Abschnitt 4

Textvorschlag der Kommission	*Ergänzung*
4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.	4. Where a transfer is based on contractual clauses as referred to in point (d) ***or (e)*** of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the ***competent*** supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the ***competent*** supervisory authority shall apply the consistency mechanism referred to in Article 57***.***

Ergänzung
Vorschlag für eine Verordnung
Artikel 42 - Abschnitt 4a (neu)

Textvorschlag der Kommission	*Ergänzung*
	4a***. To encourage the use of supplemental contractual clauses as referred to in point (e) of paragraph 2 of this Article, competent authorities may offer a data protection seal, mark or mechanism, adopted pursuant to Article 39, to controllers and processors who adopt these safeguards.***

Begründung

Die vorgeschlagene Ergänzung gibt sowohl den für die Datenverarbeitung Verantwortlichen als auch den Auftragsverarbeitern einen Anreiz, bei Datentransfers außerhalb der EU möglichst umfangreiche Datenschutzregelungen anzuwenden.

Heutzutage müssen Unternehmen routinemäßig personenbezogene Daten außerhalb der EU zur Verarbeitung in Drittländern übertragen. Die vorliegende Richtlinie (95/46) verbietet generell Datentransfers außerhalb der EU, solange die Kommission dem betreffenden Empfängerland kein „adäquates Niveau" in Datenschutzfragen zuschreibt. Wird ein solches „adäquates Niveau" nicht anerkannt, benötigen Unternehmen für Datentransfers eine Ausnahme in der Richtlinie, wie beispielsweise die von der Kommission oder den nationalen Datenschutzbehörden anerkannten „Standard-Datenschutzklauseln".

Standard-Datenschutzklauseln werden heutzutage von zahlreichen Unternehmen für Datentransfers verwendet. Sie stellen eine rechtsverbindliche Verpflichtung für Unternehmen außerhalb der EU dar, bestimmte „grundlegende" Maßnahmen zum Schutz von Daten umzusetzen, die aus der EU übertragen werden, einschließlich angemessene Sicherheitsmaßnahmen zum Datenschutz. Zudem regeln die Klauseln die Aufteilung der Haftung zwischen Datenüberträger und Datenempfänger für den Fall, dass Einzelpersonen zu Schaden kommen, und sie geben den Geschädigten Personen die Möglichkeit, gewisse Bestimmungen auch durchzusetzen.

Unseres Erachtens sollten diese grundlegenden Schutzmechanismen als ein Mindeststandard betrachtet werden. In zahlreichen Fällen kann es für Unternehmen angebracht sein, zusätzliche Mechanismen zum Datenschutz bei Datentransfers außerhalb Europas anzuwenden, d.h. die Standard-Datenschutzklauseln um noch weiter reichende Schutzmaßnahmen zu ergänzen. Die vorgeschlagene Ergänzung gibt Unternehmen die eindeutige Befugnis hierzu und schafft darüber hinaus einen Anreiz zur Einführung zusätzlicher Schutzmaßnahmen in Form eines Güte- bzw. Vertrauenssiegels, das einen Innovationsschub bewirken könnte.

Die vorgeschlagene Ergänzung hätte insbesondere zwei Folgen:

(1) die ausdrückliche Legalisierung zusätzlicher Standard-Datenschutzklauseln durch die für die Datenverarbeitung Verantwortlichen und Auftragsverarbeiter nach Maßgabe von Artikel 42(2)(b) und 42(2)(c) der Grundverordnung mit zusätzlichen vertraglichen Verpflichtungen, wodurch der Verbraucherschutz gestärkt würde; und

(2) die Ermutigung der für die Datenverarbeitung Verantwortlichen und der Auftragsverarbeiter zur Umsetzung dieser erweiterten Verpflichtungen durch die Einführung eines Güte- bzw. Vertrauenssiegels. Die Einführung des entsprechenden Siegels könnte nach Maßgabe von Artikel 39 der Grundverordnung erfolgen. (Siehe Vorschlag für eine entsprechende Ergänzung von Artikel 39 unten.)

Ergänzung
Vorschlag für eine Verordnung
Artikel 39 – Abschnitt 1 und 1a (neu)

Textvorschlag der Kommission	*Ergänzung*
1. The Member States and the Commission shall encourage***, in particular*** at European level***,*** the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and	1. The Member States and the Commission shall ***work with controllers, processors and other stakeholders to*** encourage at European level the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of

processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.	data protection provided by controllers and processors.
	1a. The data protection certifications mechanisms shall ***be voluntary, affordable, and available via a process that is transparent and not unduly burdensome. These mechanisms shall also be technology neutral and capable of global application and shall*** contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.

Begründung

Wie bereits erwähnt könnte ein Zertifizierungsverfahren Unternehmen dazu ermutigen, bei der Übertragung personenbezogener Daten außerhalb der EU zusätzliche Schutzmaßnahmen über die Standard-Datenschutzklauseln hinaus anzuwenden. Sollte das Parlament ein derartiges Zertifizierungsverfahren beschließen, so sollte das Verfahren auf die größtmögliche Beteiligung abzielen. Die Einführung von Zertifizierungen sollte für Unternehmen nicht mit übermäßigen finanziellen und bürokratischen Belastungen verbunden sein, die eine Teilnahme unattraktiv erscheinen lassen.

Die vorgeschlagene Ergänzung des Artikels 39 würde wichtige Bedingungen für die Einführung einer Zertifizierung schaffen, die gewährleisten würden, dass die für die Datenverarbeitung Verantwortlichen und Auftragsverarbeiter aller Größenordnungen einen guten Zugang zum Verfahren hätten. Zertifizierungen müssten insbesondere die folgenden Voraussetzungen erfüllen:

- *Die **Entwicklung** müsste **unter Beteiligung der Betroffenen auf EU-Ebene** erfolgen. Um effektive Mechanismen zu schaffen und eine breite Beteiligung zu fördern, sollten die Mitgliedstaaten und die Kommission mit den betroffenen Unternehmen bei der Entwicklung EU-weiter Zertifizierungen und Siegel zusammenarbeiten.*
- *Die Teilnahme sollte **freiwillig** sein. Eine verpflichtende Zertifizierung würde Innovationen behindern und den Wettbewerb bei der Entwicklung fortschrittlicher Datenschutzlösungen blockieren.*
- *Sie müssten finanziell **erschwinglich** sein. Einige Datenschutz-Zertifizierungen sind mit Kosten von bis zu 150.000 EUR verbunden, um lediglich eine bestimmte Funktion eines Produkts oder einer Dienstleistung zu zertifizieren. Derartige Kosten stellen eine Eintrittsbarriere für kleinere Dienstleister dar und lassen eine Teilnahme unattraktiv erscheinen.*
- Das Teilnahmeverfahren sollte **transparent und mit keinen übermäßigen Belastungen verbunden** sein. *Um die Beantragung und Umsetzung der Zertifizierung durch Unternehmen zu gewährleisten, darf der Erhalt der entsprechenden Güte- oder Vertrauenssiegel, die das Vertrauen der Verbraucher in die Datensicherheit stärken sollen, nicht mit übermäßigen*

bürokratischen oder sonstigen Belastungen verbunden sein.

- *Sie sollten eine **Einführung und Anerkennung auf globaler Ebene** ermöglichen. Um die mit einer Zertifizierung verbundenen Belastungen für Dienstleister zu reduzieren, sollten Zertifizierungen auch für Regulierungsbehörden in Drittländern außerhalb der EU akzeptabel und umsetzbar sein.*
- *Sie sollten **neutral** im Hinblick auf Systeme, Dienstleistungen oder Technologien sein. Ähnlich geartete Dienstleistungen und Produkte sollten den gleichen Bewertungskriterien unterliegen. Die Bevorzugung einzelner Lösungen würde zu Marktverzerrungen führen und Innovationen behindern.*

Internationale Datentransfers / Subunternehmen

I. Subunternehmen: Definition

Ergänzung
Vorschlag für eine Verordnung
Artikel 4 – Abschnitt (6a)

Textvorschlag der Kommission	*Ergänzung*
	'subprocessor' means the processor processing personal data on behalf of another processor or subprocessor.

Begründung

Datenverarbeiter geben Verarbeitungsaufträge oft an andere Unternehmen weiter, und solche Vereinbarungen stellen mittlerweile eine Routine im Kontext des Cloud Computings dar. Um sicherzustellen, dass diese Subunternehmen vom Regulierungsbereich des EU-Datenschutzregimes erfasst sind, sollten diese auch explizit in der Verordnung genannt werden – inklusive einer Definition, die das Subunternehmen klar vom originären Datenverarbeiter und Datenverantwortlichen unterscheidet.

II. Subunternehmen: Verpflichtungen

Ergänzung
Vorschlag für eine Verordnung
Artikel 26, Absatz (2)

Textvorschlag der Kommission	*Ergänzung*
(d) enlist another processor only with prior permission of the controller;	(d) enlist a ***subprocessor*** only with prior permission of the controller;

Ergänzung
Vorschlag für eine Verordnung
Artikel 26, Absatz (4a)

Textvorschlag der Kommission	*Ergänzung*
	Paragraph 2 shall not apply where a processing operation is carried out by a subprocessor and the processing is

governed by a contract or other legal act binding the subprocessor to the processor [and stipulating in particular that the subprocessor will be subject to the same obligations as those imposed by the controller on the processor pursuant to paragraph 2, taking into account the role and processing activities performed by the subprocessor.]

Begründung

Artikel 26(2)(d) der vorgeschlagenen Verordnung berücksichtigt, dass ein Verarbeiter die Dienste eines Subunternehmens in Anspruch nehmen kann. In derartigen Situationen sollte der Verarbeiter eine rechtlich verbindliche Vereinbarung eingehen. Eine solche Vereinbarung ist wichtig, um sicherzustellen dass sich die Verpflichtungen, die ein Datenverantwortlicher einem Datenverarbeiter auferlegt, auch auf das Subunternehmen auswirken.

Zu diesem Zweck sollte jede vertragliche Vereinbarung zwischen einem Verarbeiter und seinem Subunternehmen, dem Subunternehmen die gleichen Verpflichtungen auferlegen, wie diejenigen, die der Datenverantwortliche dem Datenverarbeiter auferlegt hat, insofern sich diese Verpflichtungen als relevant mit Blick auf die Aktivitäten des Subunternehmens erweisen. Dieser Ansatz wird dabei helfen, Datenverantwortliche und Datensubjekte zu schützen, indem das Subunternehmen vollständig verpflichtet sein wird, die ihm anvertrauten Daten zu schützen.

III. Subunternehmen: Standardvertragsklauseln

Ergänzung
Vorschlag für eine Verordnung
Erwägung 84

Textvorschlag der Kommission	*Ergänzung*
(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 nor to add other clauses 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	(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 ***and*** processors ***and processors and subprocessors*** to include the standard data protection clauses in a wider contract nor to add other clauses 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

subjects.	rights or freedoms of the data subjects. ***In some scenarios, it may be appropriate to encourage controllers and processors to provide even more robust safeguards via additional contractual commitments that supplement standard data protection clauses.***

Ergänzung
Vorschlag für eine Verordnung
Artikel 42 – Absatz 2(d)

Textvorschlag der Kommission	*Ergänzung*
2. (d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.	2. (d) contractual clauses between the controller or processor and the recipient of the data**, *which can be a subprocessor,*** authorised by a supervisory authority in accordance with paragraph 4.

Begründung

In der Studie „Reforming the Data Protection Package" zeigt das Policy Department des Europäischen Parlaments, dass im vorliegenden Entwurf der Grundverordnung Standard-Datenschutzklauseln nicht auf Vereinbarungen zwischen Auftragsverarbeitern und deren Subbeauftragten ausgeweitet werden. Wie aus der Studie hervorgeht, könnte die bestehende Lücke eine erhebliche Benachteiligung europäischer Unternehmen bewirken, einschließlich neuer Start-Ups im Technologiesektor. Die Arbeitsgruppe zu Artikel 29 stellt zudem fest, dass im Hinblick auf übertragene Daten die gleichen Verpflichtungen für Subbeauftragte gelten müssen, wie sie auch für Auftragsverarbeiter gelten.

Die vorgeschlagene Ergänzung soll die bestehende Lücke schließen. Auftragsverarbeiter delegieren die Verarbeitung von Daten oftmals an Subbeauftragte, und derartige Vereinbarungen sind Standard im Cloud Computing. Ohne Standardklauseln -- die ein zentrales Mittel zur Ermöglichung internationaler Datentransfers darstellen -- erleiden jedoch europäische Unternehmen einen Wettbewerbsnachteil, da sie ihre Subbeauftragten nicht außerhalb der EU wählen können.

Beispiel: Ein europäisches Startup-Unternehmen (Auftragsverarbeiter) könnte bei den von ihm angebotenen Leistungen auf Technologie eines Drittanbieters (Subbeauftragter) zurückgreifen. Ohne Standard-Datenschutzklauseln, die den geschützten Datenfluss an Subbeauftragte außerhalb der EU regeln, wäre das Unternehmen bei der Wahl der Plattform für seine Leistungen eingeschränkt -- und verliert dadurch möglicherweise einen Teil seiner Wettbewerbsfähigkeit.

Im Einklang mit den Empfehlungen der Studie ermöglicht die vorgeschlagene Ergänzung ausdrücklich die Ausweitung der Standard-Datenschutzklauseln auf Subbeauftragte durch die Kommission und die Mitgliedsstaaten. Dies gäbe in der EU ansässigen Anbietern von Cloud-Leistungen und anderen Marktteilnehmern mehr Flexibilität und Freiheit bei der Auswahl geeigneter Subunternehmen.

Für die Datenverarbeitung Verantwortliche / Auftragsverarbeiter

Ergänzung
Vorschlag für eine Verordnung
Artikel 4 - Punkt 5

Textvorschlag der Kommission	*Ergänzung*
(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes***, conditions and means*** of the processing of personal data; where the purposes***, conditions and means*** of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes of the processing of personal data; where the purposes of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

Ergänzung
Vorschlag für eine Verordnung
Artikel 24

Textvorschlag der Kommission	*Ergänzung*
Where a controller determines the purposes***, conditions and means*** of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.	Where a controller determines the purposes of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.

Begründung

Nach Maßgabe der vorgeschlagenen Regulierungsvorschriften sind die für die Datenverarbeitung Verantwortlichen und Auftragsverarbeiter unterschiedlichen Verpflichtungen unterworfen. Angesichts dieser Rahmenbedingungen sollte die Grundverordnung ein klares Testverfahren enthalten, mit dem Unternehmen ihren jeweiligen Status entweder als Verantwortliche für die Datenverarbeitung oder als

Auftragsverarbeiter feststellen können. Die vorgeschlagene Ergänzung würde ein solches klares Testverfahren einführen.

*Als Grundregel gilt: Während für die Datenverarbeitung Verantwortliche über den **Grund bzw. den Zweck** der Datenverarbeitung entscheiden, entscheiden Auftragsverarbeiter in der Regel über die **Art und die Konditionen** der Datenverarbeitung. Wenn beispielsweise ein Anbieter von Cloud-Diensten seinen Unternehmenskunden einen gehosteten E-Mail-Dienst anbietet, so stellt der Anbieter vermutlich einen Auftragsverarbeiter dar. Der Grund hierfür ist, dass der Anbieter lediglich über die Art der Datenverarbeitung entscheidet, d.h. er betreibt die Speicherung und Zustellung von E-Mails für die Nutzung und nach den Wünschen seiner Unternehmenskunden. Verwendet der Anbieter jedoch auch die gesammelten E-Mail-Adressen mit dem Ziel, ein Profil seiner Endbenutzer zu erstellen und Werbemails zu verschicken, so entscheidet er auch über den Grund für die Datenverarbeitung und fungiert damit als Verantwortlicher für die Datenverarbeitung. In diesem Beispiel agiert das Unternehmen als Verantwortlicher für die Datenverarbeitung für die gleichen Daten, für die er auch als Auftragsverarbeiter agiert.*

Leider unterscheidet der in der Grundverordnung vorgesehene Test nicht zwischen dem „Warum" und dem „Wie" der Datenverarbeitung. Hierdurch wird es Unternehmen erschwert, ihre Rolle als Verantwortlicher für die Datenverarbeitung oder als Auftragsverarbeiter zu bestimmen. Die Grundverordnung definiert die Verantwortlichen für die Datenverarbeitung als diejenigen Teilnehmer, die nicht nur über den „Zweck" der Datenverarbeitung (d.h. das „Warum"), sondern auch über die „Konditionen und Mittel" der Verarbeitung (d.h. das „Wie") entscheiden. Wie auch aus der Studie des Europäischen Parlaments hervorgeht, liefert dieser Ansatz kein klares Ergebnis.

Die vorgeschlagene Ergänzung würde diese Unklarheit ausräumen, indem der Bezug auf „Konditionen und Mittel" der Datenverarbeitung gelöscht und klargestellt wird, dass als Verantwortlicher für die Datenverarbeitung nur gilt, wer den „Zweck" der Verarbeitung bestimmt, d.h. der Teilnehmer, der über das „Warum" der Verarbeitung entscheidet. Diese Anpassung würde zur besseren Unterscheidung der wichtigen Rollen des Verantwortlichen für die Datenverarbeitung bzw. des Auftragsverarbeiters und damit zu einer verbesserten Rechtssicherheit beitragen.

Darüber hinaus würde die Ergänzung auch Artikel 24 (gemeinsam Verantwortliche für die Datenverarbeitung) im Einklang mit der neuen Definition gemäß Artikel 4 anpassen.

Ergänzung
Vorschlag für eine Verordnung
Artikel 26 – Abschnitt 5

Textvorschlag der Kommission	*Ergänzung*
5. 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	***deleted***

the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.

Begründung

Aus dem Vertrag von Lissabon geht eindeutig hervor, dass die Delegation von Rechtsakten als ergänzendes oder erweitertes Verfahren für nicht essenzielle Rechtsfragen gedacht ist. Im Kontext der vorgeschlagen Grundverordnung scheint die Kommission jedoch auf dem Wege der delegierten Rechtsakte in zahlreichen rechtlichen Kernfragen Einfluss auf Umfang und Anwendbarkeit zu nehmen -- einschließlich in fundamentalen Fragen wie beispielsweise die Pflichten von Auftragsverarbeitern (Artikel 26(5)).

Die Pflichten von Auftragsverarbeitern sollten jedoch in der eigentlichen Verordnung klar definiert werden. Europäische Auftragsverarbeiter -- ebenso wie die Verantwortlichen für die Datenverarbeitung und Datensubjekte, in deren Dienst sie stehen -- sollten nicht auf spätere sekundäre Gesetzgebung bei der Festlegung ihrer Verantwortlichkeiten, Pflichten und Aufgabenfelder angewiesen sein. Aus diesem Grund schlagen wir die Löschung von Artikel 26(5) vor.

Zentrale Anlaufstelle für den Datenschutz / „Hauptniederlassung“

Ergänzung
Vorschlag für eine Verordnung
Artikel 4 - Punkt 13

Textvorschlag der Kommission	*Ergänzung*
(13) ‘main establishment’ means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration in the Union;	(13) ‘main establishment’ means as regards the controller, ***including a controller that is also a processor,*** the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor ***that is not also a controller,*** 'main establishment' means the place of its central administration in the Union;

Ergänzung
Vorschlag für eine Verordnung
Erwägung 27

Textvorschlag der Kommission	*Ergänzung*
(27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute	(27) The main establishment of a controller in the Union, ***including a controller that is also a processor,*** should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and

such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.	technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor ***that is not also a controller*** should be the place of its central administration in the Union.

Begründung

Derzeit unterliegen EU-weit operierende Unternehmen potenziell 27 unterschiedlichen nationalen Regulierungsbehörden. Der vorliegende Entwurf schafft hier deutliche Abhilfe, indem Unternehmen, die innerhalb der EU Daten verarbeiten, nur einer einzigen Aufsichtsbehörde am Sitz ihrer „Hauptniederlassung" unterliegen sollen („One Stop Shop"-Ansatz). Wie auch das Europäische Parlament festgestellt hat, ist dies ein wichtiger Schritt bei der Bildung eines echten gemeinsamen Marktes für personenbezogene Daten, bei dem „Kosten gesenkt, eine einheitliche Anwendung gewährleistet und die Rechtssicherheit gestärkt werden".

Leider sieht der aktuelle Entwurf jedoch bei der Bestimmung der Hauptniederlassung unterschiedliche Tests für die Verantwortlichen für die Datenverarbeitung und für Auftragsverarbeiter vor. Dieser Ansatz ignoriert die Tatsache, dass einige der für die Datenverarbeitung Verantwortlichen gleichzeitig als Auftragsverarbeiter fungieren. (Beispiel: Ein Anbieter von Cloud-Diensten bietet seinen Kunden einen gehosteten E-Mail-Dienst an, aber sammelt gleichzeitig E-Mail-Adressen, um eigene Dienstleistungen zu erbringen. In diesem Szenario fungiert der Anbieter als Verantwortlicher für die Datenverarbeitung für die gleichen Daten, bei denen er als Auftragsverarbeiter agiert.) In einem solchen Fall ergibt es keinen Sinn, unterschiedliche Tests zur Bestimmung der zuständigen Regulierungsbehörde durchzuführen, da die betreffenden Unternehmen in diesem Fall erneut unterschiedlichen nationalen Regulierungsbehörden in unterschiedlichen Mitgliedsstaaten unterstehen würden.

Die vorgeschlagene Ergänzung stellt eher eine angemessene Lösung vor, da sie den gleichen Test für die Verantwortlichen für die Datenverarbeitung und Auftragsverarbeiter in den Fällen vorsieht, bei denen ein Unternehmen in beiden Rollen agiert. Dieser Ansatz gewährleistet, dass die entsprechenden Verantwortlichen für die Datenverarbeitung in vollem Umfang vom geplanten „One Stop Shop"-Ansatz profitieren können, der das Kernstück des vorliegenden Entwurfs darstellt.

Verletzungen des Datenschutzes

Ergänzung
Vorschlag für eine Verordnung
Artikel 31 – Abschnitt 1

Textvorschlag der Kommission	*Ergänzung*
1. In the case of a personal data breach, the controller shall without undue delay ***and, where feasible, not later than 24 hours after having become aware of it,*** notify the personal data breach to ***the*** supervisory authority. ***The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.***	1. In the case of a personal data breach ***that is likely to lead to significant risk of substantial harm to a data subject***, the controller shall without undue delay notify the personal data breach to ***its competent*** supervisory authority.

Amendment
Proposal for a regulation
Article 32 – paragraph 1

Textvorschlag der Kommission	*Ergänzung*
1. When the personal data breach is likely to ***adversely affect the protection of the personal data or privacy of*** the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.	1. ***Upon determination by the competent supervisory authority,*** when the personal data breach is likely to ***lead to significant risk of substantial harm to*** the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.

Begründung

Mit den vorgeschlagenen Ergänzungen wären die für die Datenverarbeitung Verantwortlichen nur zur Mitteilung bei schwerwiegenden Verletzungen verpflichtet. Die Verpflichtung zur Mitteilung bereits unerheblicher Verletzungen könnte ungewollte Nebeneffekte nach sich ziehen: Zunächst einmal könnte eine solche Regelung zu übertriebener Sorge bei Datensubjekten führen, und letztlich könnten alle Mitteilungen einfach ignoriert werden. Eine Verpflichtung zur Anzeige harmloser Verstöße würde zudem zu einer unnötigen Mehrbelastung der Datenschutzbehörden führen und auf lange Sicht die Kosten für europäische Unternehmen erhöhen. Um eine gesunde und vertrauenswürdige Online-Umgebung zu gewährleisten, sollten Verstöße gegen datenschutzrechtliche Bestimmungen im Einklang mit ihrem Schadenspotenzial behandelt werden. Es erscheint nicht sinnvoll, einen geringfügigen Verstoß mit

geringem Schadenspotenzial für die Betroffenen (z.B. ein gehacktes Spielerkonto, bei dem der Eindringling Zugriff auf die Spielstände des Betroffenen erhält) einem Verstoß gleichzusetzen, bei dem ein erhebliches Risiko schwerwiegender Schäden besteht (z.B. wenn sensitive personenbezogene medizinische Daten betroffen sind).

Die vorgeschlagene Ergänzung zu Artikel 31 sieht auch die Löschung der Mitteilungsfrist binnen 24 Stunden vor, die sowohl von Unternehmen als auch von Regulierungsbehörden als unrealistisch angesehen wird. Die für die Datenverarbeitung Verantwortlichen brauchen mehr Zeit, um Art des Verstoßes, Betroffene Personen und Schadenspotenzial für die betroffenen Datensubjekte festzustellen.

Hinweis: Erwägung 67 müsste entsprechend angepasst werden.

Ergänzung
Vorschlag für eine Verordnung
Artikel 31 a (neu)

Textvorschlag der Kommission	*Ergänzung*
	Notification of a personal data breach shall not be required if the controller demonstrates to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

Begründung

Die Mitteilung jeder einzelnen Verletzung, auch in Fällen ohne ernsthaftes Schadenspotenzial, hätte Praxisuntauglichkeit, unverhältnismäßige Kosten und Undurchführbarkeit des Systems zur Folge. Darüber hinaus könnte es zu übertriebener Besorgnis bei den Datensubjekten und sowohl bei den Verantwortlichen für die Datenverarbeitung als auch bei Datenschutzbehörden zu zusätzlichen Kosten führen. Um sicherzustellen, dass nur schwerwiegende Verstöße mitgeteilt werden, sollte keine Mitteilungspflicht in Fällen bestehen, in denen Daten für den Eindringling unlesbar werden, beispielsweise infolge technischer Schutzmaßnahmen wie Verschlüsselung, De-Identification etc.

Verwaltungstechnische Sanktionen

Ergänzung
Vorschlag für eine Verordnung
Artikel 79

Textvorschlag der Kommission	*Ergänzung*
1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.	1. Each ***competent*** supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.
2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach and the degree of co-operation with the supervisory authority in order to remedy the breach	2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, ***the sensitivity of the data in issue,*** the intentional or negligent character of the infringement, ***the degree of harm or risk of significant harm created by the violation,*** the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach. ***In setting an administrative fine, supervisory authorities shall also take into account fines, damages or other penalties previously imposed by a court or other body on the natural or legal person in respect of the violation in issue.***
	2a. Aggravating factors that support administrative fines at the upper limits established in paragraphs 4 to 6 shall include in particular:
	(i) repeated violations committed in reckless disregard of applicable law,
	(ii) refusal to co-operate with or obstruction of an enforcement process, and

	(iii) violations that are deliberate, serious and likely to cause substantial damage.
	2b. Mitigating factors which support administrative fines at the lower limits established in paragraphs 4 to 6 shall include:
	(i) measures having been taken by the natural or legal person to ensure compliance with relevant obligations,
	(ii) genuine uncertainty as to whether the activity constituted a violation of the relevant obligations,
	(iii) immediate termination of the violation upon knowledge, and
	(iv) co-operation with any enforcement processes.
	(v) negligent violations characterised by a simple failure to act with due care, and not by intent.
3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, ***where:***	3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed.
(a) a natural person is processing personal data without a commercial interest; or	
(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.	
4. The supervisory authority ***shall*** impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, ***intentionally or negligently***: ….	4. The supervisory authority ***may, in its discretion,*** impose a ***total*** fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover ***up to a maximum of 500 000 EUR per case***, to anyone who, ***in deliberate violation of law or with reckless disregard for applicable***

	obligations: . . . .
5. The supervisory authority ***shall*** impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, ***intentionally or negligently****:*	5. The supervisory authority ***may, in its discretion,*** impose a ***total*** fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, ***up to a maximum of 1 000 000 EUR per case***, to anyone who, ***in deliberate violation of law or with reckless disregard for applicable obligations***: . . . .
6. The supervisory authority ***shall*** impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, ***intentionally or negligently***:	6. The supervisory authority ***may, in its discretion,*** impose a ***total*** fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover ***up to a maximum of 2 000 000 EUR per case***, to anyone who, ***in deliberate violation of law or with reckless disregard for applicable obligations***: . . . .
The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.	***Where evidence exists to demonstrate the continued failure of the sanctions established in paragraphs 1 to 6 of this Article to address serious abuses, t***he Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.

Begründung

Um eine gesunde und sichere Online-Umgebung zu gewährleisten, müssen Unternehmen für Verstöße gegen gesetzliche Regelungen zur Verantwortung gezogen werden. Während jedoch vorsätzliche und

rücksichtslose Verstöße gegen den vorliegenden Entwurf mit erheblichen Bußen geahndet werden sollten, wäre es unverhältnismäßig und wenig sinnvoll, die gleichen Strafen bei unbeabsichtigten Verstößen zu verhängen. In der aktuellen Fassung unterscheidet der Entwurf nicht zwischen fahrlässigen und vorsätzlichen Verstößen, was zu Problemen bei der Durchsetzung führen dürfte. Vorsätzliche oder rücksichtslose Verstöße sollten sicherlich strenger geahndet werden als Verfehlungen infolge von Fahrlässigkeit. Zusammengenommen sollen die vorstehend beschriebenen Ergänzungen gewährleisten, dass verhängte Sanktionen in Relation zum Tatbestand stehen, und dass die strengsten Sanktionen für schwerwiegende Verstöße vorgesehen sind.

Für den Erfolg der Grundverordnung ist es von zentraler Bedeutung, dass die Aufsichtsbehörden bei der Durchsetzung der Ziele der Verordnung alle erforderlichen Mittel an der Hand haben. Die vorgeschlagenen Ergänzungen ermöglichen es den Aufsichtsbehörden, im eigenen Ermessen abschreckende Sanktionen zu verhängen, wobei gleichzeitig die schwersten Sanktionen für besonders schwerwiegende Fälle vorbehalten sind.

Darüber hinaus sollten die Ergänzungen auch gewährleisten, dass Sanktionen nur durch die jeweils zuständige Aufsichtsbehörde verhängt werden. Wenn ein- und derselbe Verstoß mehrfach durch unterschiedliche Datenschutzbehörden geahndet werden könnte, hätte dies einen abschreckenden Effekt auf Unternehmen. Die Folge wäre ein Rückgang der Investitionen in technologieorientierte Unternehmen. Die vorgeschlagene Ergänzung würde verhindern, dass Unternehmen für die gleiche Verfehlung mehrfach durch bis zu 27 verschiedene Datenschutzbehörden bestraft werden könnten, was außerdem dem Ansatz einer einzigen verantwortlichen Anlaufstelle für Datenschutzfragen widersprechen würde.

Delegierte Rechtsakte

Ergänzung
Vorschlag für eine Verordnung
Artikel 86 – Abschnitt 2

Textvorschlag der Kommission	*Ergänzung*
2. The delegation of power referred to in ***Article 8(3), Article 9(3),*** Article 12(5), Article 14(7), Article 15(3), ***Article 17(9),*** Article 20(6), ***Article 22(4),*** Article 23(3), ***Article 26(5),*** Article 28(5), ***Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8),*** Article 35(11), Article 37(2), Article 39(2), ***Article 43(3), Article 44(7), Article 79(7),***[3] Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.	2. The delegation of power referred to in Article 12(5), Article 14(7), Article 15(3), Article 20(6), Article 23(3), Article 28(5), Article 35(11), Article 37(2), Article 39(2), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

Ergänzung
Vorschlag für eine Verordnung
Artikel 86 – Abschnitt 3

Textvorschlag der Kommission	*Ergänzung*
3. The delegation of power referred to in ***Article 8(3), Article 9(3),*** Article 12(5), Article 14(7), Article 15(3), ***Article 17(9),*** Article 20(6), ***Article 22(4),*** Article 23(3), ***Article 26(5),*** Article 28(5), ***Article 30(3)***, ***Article 31(5), Article 32(5), Article 33(6), Article 34(8),*** Article 35(11), Article 37(2), Article 39(2), ***Article 43(3), Article 44(7), Article 79(7),*** Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified	3. The delegation of power referred to in Article 12(5), Article 14(7), Article 15(3), Article 20(6), Article 23(3), Article 28(5), Article 35(11), Article 37(2), Article 39(2), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

[3] *Note that this Article is mis-cited in the proposed Regulation as Article 79(6). The correct reference is to Article 79(7).*

therein. It shall not affect the validity of any delegated acts already in force.	

Ergänzung
Vorschlag für eine Verordnung
Artikel 86 – Abschnitt 4

Textvorschlag der Kommission	*Ergänzung*
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	4. ***The Commission shall present proposals for delegated acts to be adopted pursuant to Article 12(5), Article 14(7), Article 15(3), Article 20(6), Article 23(3), Article 28(5), Article 35(11), Article 37(2), Article 39(2), Article 81(3), Article 82(3) and Article 83(3) within two years of the date of publication of this Regulation in the Official Journal of the European Union.*** As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

Ergänzung
Vorschlag für eine Verordnung
Artikel 86 – Abschnitt 5

Textvorschlag der Kommission	*Ergänzung*
5. A delegated act adopted pursuant to ***Article 8(3), Article 9(3),*** Article 12(5), Article 14(7), Article 15(3), ***Article 17(9),*** Article 20(6), ***Article 22(4),*** Article 23(3), ***Article 26(5),*** Article 28(5), ***Article 30(3)***, ***Article 31(5), Article 32(5), Article 33(6), Article 34(8),*** Article 35(11), Article 37(2), Article 39(2), ***Article 43(3), Article 44(7), Article 79(7),*** Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European	5. A delegated act adopted pursuant to Article 12(5), Article 14(7), Article 15(3), Article 20(6), Article 23(3), Article 28(5), Article 35(11), Article 37(2), Article 39(2), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.

Parliament or the Council.

Begründung

Von den 91 Artikeln im Entwurf der Grundverordnung sehen 26 die Delegation von Rechtsakten an die Kommission vor. Jede vorgesehene Delegation von Rechtsakten autorisiert die Kommission dazu, neue rechtliche Grundlagen auf sekundärer Ebene zu schaffen, die EU-weit gültig wären.

Die hohe Zahl der vorgesehenen delegierten Rechtsakte hätte zur Folge, dass Unternehmen auch nach Einführung der Grundverordnung noch über viele Jahre hinweg mit stets neuen Bestimmungen zu rechnen hätten. Dies erschwert es Daten verarbeitenden Unternehmen, einen Überblick über ihre Verpflichtungen zu behalten. Zudem führt es zu Verwirrung im Hinblick auf die Rechte von Datensubjekten. Derart unsichere regulatorische Verhältnisse hätten einen negativen Effekt auf europäische Internetunternehmen, insbesondere auf Start-Ups und weniger etablierte Unternehmen, die bei der Suche nach langfristigen Investoren auf einen konsistenten und nachhaltigen regulatorischen Rahmen angewiesen sind. Studien haben gezeigt, dass kleinere und mittlere Unternehmen oftmals unverhältnismäßig stark unter den Kosten für die Einhaltung regulatorischer Vorgaben zu leiden haben.

Während in einigen Fällen die Delegation von Rechtsakten erforderlich sein könnte, um bestimmte Aspekte der Grundverordnung besser abzugrenzen, sollte die Kommission darauf bedacht sein, Anzahl und Ausmaß derartiger delegierter Rechtsakte bewusst zu begrenzen. Vor diesem Hintergrund sollte die Zahl der delegierten Rechtsakte erheblich reduziert werden, und wo erforderlich, sollten delegierte Rechtsakte mit einem konkreten Zeitrahmen für die Umsetzung versehen werden. Wir verweisen insbesondere auf die folgenden Punkte:

1. ***Im Einklang mit dem Vertrag von Lissabon sollten Bestimmungen zur Delegation von Rechtsakten gelöscht werden, sofern sie essenzielle rechtliche Fragen betreffen.*** *Zahlreiche der vorgesehenen Delegationen von Rechtsakten -- darunter Artikel 9(3), Artikel 22(4), Artikel 26(5), Artikel 31(5), Artikel 32(5), Artikel 33(6), Artikel 34(8), Artikel 43(3), Artikel 44(7) sowie Artikel 79(7) -- betreffen essenzielle Aspekte des gesamten datenschutzrechtlichen Rahmens. Nach Maßgabe des Vertrags von Lissabon sollten delegierte Rechtsakte jedoch eine unterstützende Funktion bei nicht essenziellen rechtlichen Fragen haben. Essenzielle rechtliche Fragestellungen sollten direkt in der Grundverordnung angesprochen und nicht auf einen späteren Zeitpunkt verschoben werden.*

2. ***Im Einklang mit etablierter EU-Politik sollten diejenigen Delegationen von Rechtsakten gelöscht werden, die der Kommission die Möglichkeit geben würden, die technologische Entwicklung zu diktieren.*** *Einige der vorgesehenen Delegationen von Rechtsakten -- darunter Artikel 8(3), Artikel17(9) und Artikel 30(3) -- könnten das in der EU etablierte Prinzip der Technologieneutralität gefährden, indem die Kommission zur Festlegung von Regeln, Standards oder Formaten befugt würde. Aufgrund der Geschwindigkeit bei der Weiterentwicklung von Technologien sind neue Vorschriften oftmals bereits veraltet, bevor sie überhaupt umgesetzt werden. Um dieses Szenario zu vermeiden, sollte die Kommission ihren Fokus auf das „Was" legen und der Technologiebranche und den Märkten die Entscheidung beim „Wie" überlassen.*

Die Umsetzung delegierter Rechtsakte, die in die Grundverordnung aufgenommen werden, sollte einem klaren Zeitplan unterliegen. *Ohne klaren Zeitplan für die Umsetzung delegierter Rechtsakte*

wären die für die Datenverarbeitung Verantwortlichen sowie Auftragsverarbeiter und Datensubjekte auf unbestimmte Zeit einem hohen Maß an Unsicherheit bezüglich ihrer Rechte und Pflichten unterworfen. Auch die Arbeitsgruppe zu Artikel 29 beklagt diesen Aspekt und fordert die Kommission in ihrer Stellungnahme auf, zumindest anzugeben, welche der delegierten Rechtsakte jeweils kurz-, mittel- und langfristig umgesetzt werden sollen.
Entsprechende Anpassungen wären erforderlich für Erwägung 129 und Erwägung 131 sowie Artikel 6(5), Artikel 8(3), Artikel 9(3), Artikel 17(9), Artikel 22(4), Artikel 26(5), Artikel 30(3), Artikel 31(5), Artikel 32(5), Artikel 33(6), Artikel 34(8), Artikel 43(3), Artikel 44(7), und Artikel 79(7).

Rechenschaftspflicht

Ergänzung
Vorschlag für eine Verordnung
Artikel 22 – Verantwortlichkeiten des für die Datenverarbeitung Verantwortlichen

Textvorschlag der Kommission	*Ergänzung*
1.The controller shall ***adopt policies and*** implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.	1. The controller, ***or the group of undertakings of which the controller is a member,*** shall implement appropriate measures to ensure and be able to demonstrate ***upon request*** that the processing of personal data is performed in compliance with this Regulation.
2. The measures provided for in paragraph 1 shall in particular include:	2. The measures provided for in paragraph 1 shall in particular include:
(a) keeping the documentation pursuant to Article 28;	***(a) management commitment and oversight to ensure processing of personal data is carried out in compliance with this Regulation, including, if appropriate, the appointment of the Data Protection Officer pursuant to Article 35.1;***
(b) implementing the data security requirements laid down in Article 30;	***(b) policies and procedures that document the requirements of this Regulation including the security requirements laid down in Article 30;***
(c) performing a data protection impact assessment pursuant to Article 33;	(c) ***an assessment of risks associated with the processing of personal data such as, but not limited to, data protection impact assessments as required under Article 33;***
(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);	***(d) appropriate documentation of processing activities as laid out in Article 28;***
(e) designating a data protection officer pursuant to Article 35(1).	(e) ***making appropriate summaries of its policies and procedures available to the relevant supervisory authority upon request, responding expeditiously to inquiries, complaints and requests from data subjects to access and where appropriate, to rectify, block or erase data the processing of which does not comply with the provisions of this***

legislation, in particular because of the incomplete or inaccurate nature of the data, and offering a recourse mechanism when harm occurs to a data subject due to a failure to comply with its policies and procedures; such measures shall be proportional to the nature and volume of the personal data that the controller processes, the nature of such processing, and the risks to the rights and freedoms of data subjects represented by such processing.

Begründung

Im Einklang mit den Empfehlungen der Artikel 29 Datenschutzgruppe (WP 173) führt diese Ergänzung Rechenschaftspflichten in den regulatorischen Rahmen ein. Wie von der Arbeitsgruppe anerkannt, helfen Rechenschaftspflichten sich „von der Theorie zur Praxis" zu bewegen, indem sie von Datenverantwortlichen, und durch Verarbeitungsverträge auch von Verarbeitern fordern, bedeutende und konkrete Maßnahmen zu treffen und umzusetzen, um Daten zu schützen. Insbesondere sollten schriftliche Vorgehensweisen, Prozesse und Kontrollen eingeführt werden, um sicherzustellen, dass diese Maßnahmen und Prozesse effektiv umgesetzt werden, um angemessene Zusammenfassungen dieser Maßnahmen der verantwortlichen Aufsichtsbehörde zugänglich zu machen, um angemessene Sicherheitsmaßnahmen zu ergreifen.

Die meisten globalen Unternehmen haben globale Programme zur Datenschutzeinhaltung, die auf der globalen Unternehmensebene festgelegt werden, anstatt für jeden einzelnen Datenverantwortlichen. Darüber hinaus sollte der Maßnahmenkatalog flexibler ausgestaltet sein, sodass dieser aufzeigt, was eine effektive Einhaltung bedeutet, ohne bei jedem einzelnen Punkt zu beschreibend ins Detail zu gehen. Um über das gesamte Spektrum aller Einheiten zu funktionieren, die mit Daten umgehen, sollten die relevanten Verpflichtungen verhältnismäßig und skalierbar sein, abhängig von der Art des Prozesses, des Datentyps und den vorhandenen Risiken.