FIfF Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Stellungnahme des FIfF e.V. zur Datenschutz-Grundverordnung

Wir beziehen uns auf den Entwurf einer Datenschutzgrundverordnung für Europa vom 25.1.2012 KOM(2012) 11 endgültig 2012/0011 (COD) (im Folgenden auch Kommissionsentwurf oder Grundverordnung)
und die Änderungsvorschläge des Berichterstatters Jan Philipp Albrecht vom 17.12.2012 PR\922387DE.doc PE501.927v01-00.

Das FIfF (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung) e.V. als Organisation kritischer Informatikerinnen und Informatiker
– Kennnummer im Transparenzregister: 346734610616-28 –
befürwortet den vorgelegten Entwurf der EU-Kommission zur Modernisierung des Datenschutzes, eine solche Initiative war überfällig. Wir befürworten ebenfalls die Änderungsvorschläge des Berichterstatters, insbesondere die Grundrechte-Schutzklausel im Änderungsantrag 1: „Die Mitgliedstaaten sind nach der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) verpflichtet, dafür Sorge zu tragen, dass solche Datenströme angemessen reguliert werden."

Durch die Einführung europaweit einheitlicher Standards wird endlich das EU-weite Datenschutzniveau gestärkt, auch wenn wir noch Änderungsbedarf sehen. Mit unseren Vorschlägen wollen wir für eine weitere Verbesserung sorgen und gleichzeitig unsere Erwartung bekräftigen, dass die europäische Datenschutz-Grundverordnung keinesfalls wegen wirtschaftlicher Interessen eingeschränkt werden darf. Das Grundrecht auf Datenschutz muss verstanden werden als ein Grundrecht auf informationelle Selbstbestimmung.

Mit unseren Vorschlägen zu strukturellen und Textänderungen wenden wir uns an die befassten Ausschüsse des Europäischen Parlaments.

Inhalt

1.Für eine weitere Präzisierung der Einwilligung 3
2.Für eine höhere Bewertung von Interessen der Betroffenen gegenüber den „berechtigten Interessen“ des Verantwortlichen 4
3.Für verbesserte Dokumentationspflichten 5
4.Für die Beschränkung von Profiling und Ausweitung der Informationspflicht 5
5.Für eine Orientierung an konkreten Schutzzielen bei der Umsetzung von Datenschutz durch Technik und datenschutzfreundlichen Voreinstellungen 6
6.Für angemessene Garantien beim Grenzübertritt mit mobilen Geräten 8
7.Für eine grundsätzliche Verpflichtung zu anonymisieren oder zu pseudonymisieren 9
8.Zur Ausnahme von Polizei und Justiz von der Verordnung 10
9.Für eine verpflichtende Folgenabschätzung 10
10.Für eine Begrenzung der delegierten Rechtsakte 12
11.Für eine stärkere Unabhängigkeit der Aufsichtsbehörden und Datenschutzbeauftragten 13
12.Für die Verpflichtung eines Datenschutzbeauftragten auch in kleineren Unternehmen 14
13.Zur Erhebung politischer Einstellungen durch Parteien 15
14.Für die Regelung des Beschäftigten-Datenschutzes durch die Mitgliedstaaten 15

1. Für eine weitere Präzisierung der Einwilligung

Das FIfF begrüßt ausdrücklich die Präzisierung des Einwilligungs-Begriffs in der Verordnung, insbesondere die *explizite* und *eindeutige* Einwilligung sowie das Recht auf Widerruf und Widerspruch. Die Regelungen stellen eine eindeutige Verbesserung dar und dürfen weder außen- noch binnenwirtschaftlichen Interessengruppen zuliebe abgeschwächt werden.

Das FIfF fordert

⇒ Erwägungsgrund 33. Wir unterstützen den Änderungsvorschlag des Berichterstatters: Die Verwendung von *Voreinstellungen, die die betroffene Person verändern muss, um der Verarbeitung zu widersprechen,* wie etwa standardmäßig angekreuzte Kästchen, drückt *keine freie Zustimmung* aus.

⇒ Art. 7: Da sich die technischen Bedingungen der Verarbeitung personenbezogener Daten ständig ändern, fordern wir eine *Begrenzung der Gültigkeit einer Einwilligung auf maximal vier Jahre.* Wird die Einwilligung nicht verlängert, sollte die verarbeitende Stelle verpflichtet werden, die Daten automatisch zu löschen.

⇒ Art. 8, 1: Für die wirksame Einwilligung Minderjähriger sollte *sowohl die Zustimmung der gesetzlichen Vertreter als auch die Einwilligung des einsichtsfähigen Minderjährigen* erforderlich sein.
Der Text der Verordnung wie auch der Vorschlag des Berichterstatters würde es Eltern oder rechtlichen Vertretern des Kindes ermöglichen, ohne Zustimmung des Kindes dessen personenbezogene Daten beispielsweise bei Facebook einzustellen.

⇒ Die Einwilligung muss immer gegenüber der verantwortlichen Stelle erklärt/abgegeben werden.

Begründung

Die Diskussionen um die Funktionsweise von Einwilligungen, insbesondere im Internet, zeigen, dass die Verordnung präzisere Festlegungen treffen sollte, die über die heutige unbefriedigende Situation hinausgehen.

Insbesondere die versuchte Melderechtsänderung in Deutschland hat gezeigt, dass Unternehmen der Werbe-Industrie mit erschlichenen Einwilligungen beim Meldeamt die Herausgabe von Adressen veranlassen könnten. Die Einwilligung ist der Struktur nach eine Ermächtigung für die verantwortliche Stelle und muss auch dort erhoben und verwaltet werden.

2. Für eine höhere Bewertung von Interessen der Betroffenen gegenüber den „berechtigten Interessen“ des Verantwortlichen

Das FIfF begrüßt ausdrücklich die Änderungen des Berichterstatters. Die Änderungsanträge 99 bis 101 enthalten eine klarere Regelung der Voraussetzungen. Sie verlangen die Unterrichtung der betroffenen Person durch den für die Verarbeitung Verantwortlichen, wobei die Gründe für den Vorrang seiner Interessen offenzulegen sind. Die Daten müssen erhoben worden sein, weil die Verarbeitung „für die Erfüllung eines Vertrages … erforderlich (ist) oder zur Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen“ (Art. 6, 1b)).

Änderungsantrag 101 nennt zusätzlich fünf Situationen, in denen die berechtigten Interessen des für die Datenverarbeitung Verantwortlichen grundsätzlich Vorrang haben.

Diese Änderungen reichen nicht aus.

Das FIfF fordert

⇒ Die Datenverarbeitungen aus *berechtigtem Interesse* sind weiter einzuschränken und insbesondere die Nutzung zu Zwecken der *Direktwerbung an die ausdrückliche Zustimmung der Betroffenen zu binden.*

⇒ Das berechtigte Interesse im Art. 6, 1b) (neu) (Änderungsantrag 101) ist auf die unter den Buchstaben a, b und d beschriebenen Fälle einzuschränken. Die Buchstaben c und e sind zu streichen.

Begründung

Wenn auch der Änderungsvorschlag eine deutliche Verbesserung gegenüber dem Kommissionsentwurf darstellt, bietet er immer noch eine breite Möglichkeit der Datenverarbeitung ohne Zustimmung.

3. Für verbesserte Dokumentationspflichten

Das FIfF begrüßt ausdrücklich die Vorschläge des Berichterstatters zur Straffung der Dokumentationspflichten und die Zusammenführung mit den Informationsrechten der Betroffenen in Art. 14. Die Änderung des Art. 37, 1a) zur Dokumentation technischer und organisatorischer Maßnahmen und Verfahren halten wir für sehr sinnvoll.

4. Für die Beschränkung von Profiling und Ausweitung der Informationspflicht

Das FIfF begrüßt ausdrücklich die Änderungen des Berichterstatters. Insbesondere die Definition von Profiling (Änderungsantrag 87) sowie die engere Fassung des Erlaubnisvorbehalts (Änderungsanträge 159, 160) geben hoffentlich mehr Rechtssicherheit. Die erweiterten Pflichten zur Auskunftserteilung (Art. 14) erlauben es den Betroffenen, ihre informationelle Selbstbestimmung zu gestalten.

Das FIfF fordert

⇒ Änderungsantrag 131 des Berichterstatters sollte erweitert werden um Angaben über Logik und Algorithmus der Profiling-Maßnahme.

⇒ Art. 20, 1 sollte wie folgt geändert werden: Eine natürliche Person hat sowohl offline als auch online das Recht, ...

⇒ Art. 20, 2a) sollte wie folgt geändert werden: ... im Rahmen des Abschlusses oder der Erfüllung eines Vertrags erforderlich ist ...

⇒ Art. 20, 3 sollte wie folgt geändert werden: Die automatisierte Verarbeitung personenbezogener Daten zum Zwecke der Auswertung bestimmter persönlicher Merkmale einer natürlichen Person darf keine in Artikel 9 genannten besonderen Kategorien personenbezogener Daten enthalten oder erzeugen, es sei denn, sie fallen unter die unter in Art. 9, 2 enthaltenen Ausnahmen.

⇒ Erwägungsgrund 58 sollte erweitert werden: Wenn Maßnahmen auf Basis von Profiling rechtmäßig erfolgen, muss dem Betroffenen die Möglichkeit eingeräumt werden, eine *zweite Meinung bei der Bewertung* einzufordern. Die Kosten hat der Verantwortliche für die Datenverarbeitung zu tragen.

Begründung

Durch Profiling entstandene Bewertungen sind nie vollständig und auch eine menschliche Beurteilung kann von Vorurteilen geprägt sein oder es können Fehlinterpretation vorliegen. Das FIfF fordert deshalb, auch Betroffenen, die in Profiling-Maßnahmen eingewilligt haben, das Recht auf eine zweite Bewertung der Profiling-Ergebnisse durch eine andere Person einzuräumen.

⇒ Artikel 20 sollte ergänzt werden durch ein generelles Verbot von Profiling-Maßnahmen, die (ungewollt oder gewollt) zu Diskriminierung führen.

⇒ Präzisierung zum Änderungsantrag 38 (Erwägungsgrund 58):
Solche Maßnahmen sollten nicht zur Diskriminierung führen; eine *Gleichbehandlung* muss *durch menschliches Eingreifen sichergestellt* werden.

Begründung

Änderungsantrag 38 zum Erwägungsgrund 58 ergänzt zwar: „Solche Maßnahmen sollten ohne menschliches Eingreifen nicht zu Diskriminierung führen". Der Satz ist aber missverständlich, denn solche Maßnahmen sollten auch *mit* menschlichem Eingreifen nicht zu Diskriminierung führen.

⇒ Diskriminierungen sind auch dann auszuschließen, wenn die Ungleichbehandlung erst durch das *Zusammenwirken einzelner Profiling-Maßnahmen* erfolgt.

Begründung

Wenn Profiling Teil größerer Prozesse ist, hat es möglicherweise keinen gesonderten Einfluss im Einzelnen, in der Summe kann es aber zu einer Beeinträchtigung oder Diskriminierung führen.

5. Für eine Orientierung an konkreten Schutzzielen bei der Umsetzung von Datenschutz durch Technik und datenschutzfreundlichen Voreinstellungen

Das FIfF begrüßt die Verpflichtung zu datenschutzfreundlicher Technikgestaltung bei Verarbeitung und Erhebung personenbezogener Daten. Wir unterstützen Änderungsantrag 177 des Berichterstatters zu Artikel 23, 2, der die betroffenen Personen in der Lage versetzt, die Verbreitung ihrer personenbezogenen Daten zu kontrollieren.

Wir unterstützen auch den Auftrag in Art. 23, 3 an den Europäischen Datenschutzausschuss, weitere Kriterien und Anforderungen an den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen festzulegen.

Folgende Verbesserungen halten wir für nötig, um das Ziel datenschutzfreundlicher Technikgestaltung konsequenter umzusetzen.

Das FIfF fordert

Die Aufnahme der *erweiterten Schutzziele* in die Verordnung.

⇒ Die *Schutzziele* sollten in Art. 5, Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten, aufgenommen werden.

Für die Definitionen empfehlen wir:

- *Transparenz* (Absatz 1 – Buchstabe a), wie vom Berichterstatter vorgeschlagen.
- *Zweckbindung* (Absatz 1 – Buchstabe b), wie vom Berichterstatter vorgeschlagen. Ergänzt werden sollte der Satz: „Sie dürfen nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können."

- *Datensparsamkeit* (Absatz 1 – Buchstabe c). Der vom Berichterstatter vorgeschlagene Begriff der Datenminimierung sollte durch Datensparsamkeit ersetzt werden.
- *Integrität* (Absatz 1 – Buchstabe d), wie vom Berichterstatter vorgeschlagen.
- Der Begriff *Speicherminimierung* sollte durch *Datensparsamkeit* ersetzt werden und zusätzlich der Begriff der Zweckbindung eingefügt werden (Absatz 1 – Buchstabe e).
- Der vom Berichterstatter vorgeschlagene Begriff der *Eingriffsmöglichkeit* (Absatz 1 – Buchstabe e a (neu)) sollte durch den in der Informationssicherheit üblichen Begriff der Intervenierbarkeit ersetzt werden.
- Im vom Berichterstatter vorgeschlagenen Änderungsantrag 98, Art. 5 – Absatz 1 a (neu) sollte der Begriff operationelle Maßnahmen durch *organisatorische Maßnahmen* ersetzt werden.

⇒ Vertraulichkeit und Verfügbarkeit sind nur in Erwägungsgrund 39 beschrieben. Sie sollten in Art. 5 Absatz 1 unter einem zusätzlichen Buchstaben erwähnt werden, wie etwa:

- [Personenbezogene Daten müssen] so verarbeitet werden, dass nur befugte Personen auf Verfahren und Daten zugreifen können *(Vertraulichkeit)* und Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können *(Verfügbarkeit).* Es muss sichergestellt werden, dass Verfahren nur zweckgebunden eingesetzt werden und eine klare Zwecktrennung zu verwandten Verfahren besteht *(Zweckbindung)*.

⇒ Die Schutzziele sollten in Erwägungsgrund 61 aufgenommen werden.

⇒ Die Formulierung des Berichterstatters in Erwägungsgrund 61 „zum Schutz der Privatsphäre“ sollte durch „zum Schutz der personenbezogenen Daten“ ersetzt werden. Die Begriffe *Datenminimierung* und *Zweckbeschränkung* sollten durch die Begriffe *Datensparsamkeit* und *Zweckbindung* ersetzt werden.

Begründung

Datenschutzfreundliche Technikgestaltung wird in der Informationssicherheit in Schutzziele übersetzt. Dies sind Vertraulichkeit, Integrität, Verfügbarkeit sowie die *erweiterten Schutzziele* der Transparenz für die Betroffenen, Zweckbindung ihrer personenbezogenen Daten, und Intervenierbarkeit als Eingriffsmöglichkeit der Betroffenen in Ausübung ihrer Rechte. Auch die erweiterten Schutzziele sind in technischen und organisatorischen Prozessen umzusetzen und sollten daher ebenfalls, etwa in einem gesonderten Erwägungsgrund aufgenommen werden.

Das FIfF fordert außerdem

Die *Verpflichtung der Hersteller zu Datenschutz durch Technik und datenschutzfreundlichen Voreinstellungen,* etwa durch verpflichtende Zertifizierungsverfahren der Hersteller. Solche obligatorischen Zertifizierungsverfahren sind durch eine EU-Institution zu kontrollieren. Eine datenschutzfreundliche Technik muss die gesamten Prozesse in den Blick nehmen.

⇒ In Erwägungsgrund 61 sollten *verpflichtende Verhaltenskodices, Siegel* und *Zertifizierungsverfahren* gemäß Art. 38 und 39, 1 aufgenommen werden, wenn besondere Kategorien personenbezogener Daten oder solche von Kindern verarbeitet werden oder wenn mit den Verfahren Profile erstellt

werden. Solche obligatorischen Zertifizierungsverfahren sind durch eine EU-Institution zu kontrollieren.

Begründung

Ein effektiver Schutz ist nur möglich, wenn *in allen Phasen der Herstellung und Nutzung* von Produkten und Dienstleistungen auf die datenschutzfreundliche Gestaltung geachtet wird. Dabei ist sicherzustellen, dass alle Prozesse bei Entwicklung und Nutzung der IT-Systeme an den Schutzzielen ausgerichtet sind und sie erfüllen: Systementwicklungsprozesse, Datenschutzprozesse und Geschäftsprozesse, in denen die IT-Systeme fachlich genutzt werden.

Deshalb sind die Ergänzungen durch den Berichterstatter außerordentlich wichtig, bereits bei den Herstellern anzusetzen und Regelungen sowie Anreize für eine datenschutzfreundliche Technik zu schaffen.

6. Für angemessene Garantien beim Grenzübertritt mit mobilen Geräten

Das FIfF begrüßt ausdrücklich, dass die Verordnung in den Art. 25, 26 und 27 für Unternehmen eine neue *Ortsbindung, Zweckbindung* und *Transparenz* fordert, die sich auch am Unternehmensort der meisten Dienste-Nutzer orientieren und eine Bindung an die europäische Gesetzgebung verpflichtend machen. Das ist ein erster, sehr guter Schritt.

Das FIfF teilt die Ansicht des Berichterstatters, dass die vorgeschlagene neue Option, *Verarbeitungssektoren* in Drittstaaten als angemessen anzuerkennen, *nicht wünschenswert* ist.

Das FIfF begrüßt den Änderungsantrag 53 zum Erwägungsgrund 80, in dem „bestimmte Drittländer oder bestimmte Gebiete [...] eines Drittlandes oder eine internationale Organisation“, die „keinen angemessenen Datenschutz“ bieten, von der Übermittlung personenbezogener Daten ausgeschlossen werden können, sowie Erwägungsgrund 82, der ein Verbot der Übermittlung von personenbezogenen Daten in bestimmten Fällen vorsieht.

In diesem Zusammenhang begrüßen wir auch den Änderungsantrag 54 zum Erwägungsgrund 89, in dem finanzielle Entschädigungsleistungen gefordert werden, wenn eine nicht genehmigte Verarbeitung von Daten in Drittstaaten erfolgt.

Das FIfF begrüßt den Änderungsantrag 40 des Berichterstatters zum Erwägungsgrund 60, der das Konzept der Rechenschaftspflicht erwähnt und den geforderten Nachweis verschärft.

Diese Änderungen reichen aber nicht aus.

Das FIfF fordert

⇒ in Anlehnung an Paragraf 2a) im deutschen Telemedien-Gesetz festzuschreiben, dass ein mobiler Dienste-Anbieter *nicht nur einen Vertreter sondern einen Sitz* in dem Land haben muss, in dem mehrheitlich die Vertragsnehmer der mobilen Dienstleistungen ansässig sind. Verlagert sich die Mehrzahl der Vertragsnehmer während der Dauer von zwei Jahren in einen anderen Mitgliedstaat, ist der Sitz in diesen Mitgliedstaat zu verlegen.

⇒ auch die *Speicherorte* der personenbezogenen Daten *transparent* zu machen. Insbesondere ist ein Widerspruchsrecht für Dienste-Nutzer oder Vertragsnehmer mobiler Dienste für mobile (End-)Geräte einzuräumen, wenn die *Verbindungsdaten* in Kombination *mit personenbezogenen Daten zur Abrechnung* an andere Dienste-Anbieter übermittelt werden, die ihren Sitz außerhalb der EU haben und nicht der Verordnung unterliegen.

⇒ nicht nur Profiling innerhalb von Anwendungen zu adressieren, sondern auch IT-Infrastrukturen in ihrer Gesamtheit. Dazu sollte im Erwägungsgrund 60 eine Auskunftspflicht implementiert und der letzte Satz wie folgt geändert werden: „ […] und er sollte dies auch nachweisen und *auf Anfrage des Betroffenen offenlegen* müssen."

⇒ ein *Recht* der Vertragsnehmer *auf Einsichtnahme* in übermittelte personenbezogene Daten und ein *Einspruchsrecht*, wenn bei Lastausgleich EU-grenzüberschreitend Wirknetze kooperierender Dienste-Anbieter hinzu- und abgeschaltet werden.

⇒ ein *Recht* der Vertragsnehmer darauf, dass ihre mobilen Geräte zum Schutz personenbezogener Daten *auf Antrag unbrauchbar gemacht* werden können.

⇒ eine Formulierung wie im Telemedien-Gesetz in Paragraf 13 (5), die die EU-Richtlinie 95/46/EG ergänzt, aufzunehmen: „Die Weitervermittlung zu einem anderen Dienste-Anbieter ist dem Nutzer anzuzeigen."

Begründung

Ein vergleichbarer Ansatz wie in Art. 25, 26 und 27 ist für die Übermittlung personenbezogener Daten bei der Nutzung mobiler Dienste anzustreben. Wir fordern eine entsprechende Anpassung auch für die eigenen personenbezogenen Daten, so dass grenzüberschreitend das informationelle Selbstbestimmungsrecht gewahrt bleibt.

Mit der empfohlenen Streichung im Bericht des Berichterstatters in Art. 25, 3, 3 wird die ohnehin nur indirekte Forderung nach einer Ortsbindung aufgehoben, die Dienste-Anbieter in Bezug auf Waren (hier mobile Geräte) zu gewährleisten haben. Eine zu Paragraf 2a) Telemedien-Gesetz vergleichbare Ergänzung würde dafür sorgen, dass sich der Sitz des Dienste-Anbieters nach dem Ort in der EU bestimmt, an dem seine Kunden mehrheitlich ansässig sind.

Ohne die verbriefte Forderung der Ortsbindung bleibt abzuwarten, ob die in Änderungsvorschlag 72 zu Erwägungsgrund 130 und Änderungsvorschlag 73 zu Erwägungsgrund 131 geforderten Standards und Verfahren und damit verbundene Zertifizierungen für bestimmte Drittländer oder bestimmte Gebiete eines Drittlandes oder eine internationale Organisation das Schutzbedürfnis der Betroffenen abdecken können. Möglicherweise führen diese Ansätze zu einem Aufschub und nicht zu einer Klärung in Bezug auf Ortsbindung und Transparenz.

7. Für eine grundsätzliche Verpflichtung zu anonymisieren oder zu pseudonymisieren

Das FIfF unterstützt die Änderungen des Berichterstatters in Erwägungsgrund 23 und 24, den Begriff der anonymen Daten zu spezifizieren und den Geltungsbereich der Verordnung auf pseudonyme Daten und IP-Adressen auszuweiten.

Das FIfF fordert

⇒ die *grundsätzliche Verpflichtung zur Anonymisierung bzw. Pseudonymisierung* personenbezogener Daten, sofern dies entsprechend dem Zweck der Verarbeitung möglich und angemessen ist. Wenn die Identität nicht relevant ist, muss anonymisiert werden, wenn sie relevant ist, pseudonymisiert.

⇒ Der Schutz pseudonymisierter Daten ist dem von personenbezogenen Daten gleichzustellen.

⇒ Dies schließt ein, dass die Anbieter die *Funktionen bei anonymer Nutzung nicht einschränken* dürfen und auch nicht den Eindruck erwecken dürfen, eine anonyme oder pseudonyme Nutzung sei nicht möglich.

Begründung

Es muss in der Regel möglich sein, Dienstleistungen auch ohne die Verarbeitung personenbezogener Daten in Anspruch zu nehmen oder, wenn eine eindeutige Identifikation notwendig ist, etwa im Falle sozialer Online-Netzwerke, müssen Pseudonyme möglich sein.

8. Zur Ausnahme von Polizei und Justiz von der Verordnung

Das FIfF teilt die Kritik des Berichterstatters, dass die Zusammenarbeit bei der Strafverfolgung im Vorschlag der Kommission nicht geregelt wird.

Das FIfF fordert

⇒ eine *Klärung* für Fälle wie beispielsweise, *wenn Strafverfolgungsbehörden auf geschäftliche Daten zugreifen.*

Begründung

Beim Änderungsantrag 80 zu Art. 2, 2e) gibt es (anders als im englischen Original) keinen Unterschied zwischen dem Vorschlag der Kommission und der Änderung des Berichterstatters. Die Einschränkung, dass der Ausschluss aus dem Anwendungsbereich der Verordnung nur die Tätigkeit der zuständigen Strafverfolgungsbehörden erfasst (nicht aber private Einrichtungen), war in der deutschen Fassung der Verordnung bereits enthalten.

9. Für eine verpflichtende Folgenabschätzung

Das FIfF begrüßt ausdrücklich die Änderungsvorschläge des Berichterstatters. Sie gehen aber nicht weit genug. So sollten Folgenabschätzungen für alle Profiling-Maßnahmen gelten.

Das FIfF fordert

⇒ Ergänzend zu Art. 33, 1 sollte je nach Art der Datenverarbeitung eine angemessene Abschätzung auch der längerfristigen Folgen *(über die Dauer der Datenverarbeitung hinaus)* verpflichtend sein.

⇒ Art. 33, 3b) (neu) sollte erweitert werden: eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken auch *über die Dauer der Datenverarbeitung hinaus.*

⇒ Folgeabschätzungen sollten für jede Verarbeitung besonderer personenbezogener Daten gelten. In Artikel 33, 2b) des Kommissionsentwurfs sollte deshalb „in großem Umfang“ gestrichen werden.

⇒ Die *Folgenabschätzung* sollte möglichst vollständig *veröffentlicht* und den Betroffenen vor der Einwilligung zur Verfügung gestellt werden, soweit sie nicht in Teilen Auskunft über vertrauliche interne Vorgänge enthält. Gegebenenfalls kann das Ergebnis einer Auditierung zu einem Zertifizierungsverfahren die Veröffentlichung ergänzen.

Begründung

Die enthaltene Pflicht zur Datenschutzfolgenabschätzung bei der Auftragsdatenverarbeitung in Art. 30, 2 geht nicht weit genug, da sie eine Dokumentation der Maßnahmen zur Datensicherheit nicht zwingend vorsieht und eine Meldung nur zu erwarten ist, wenn der Schutz der personenbezogenen Daten verletzt wurde.

10. Für eine Begrenzung der delegierten Rechtsakte

Das FIfF begrüßt ausdrücklich den Ansatz des Berichterstatters, nähere Regelungen anstatt über delegierte Rechtsakte der EU-Kommission durch den *Europäischen Datenschutzausschuss* regeln zu lassen. Das ist ein wesentlicher Schritt in die richtige Richtung, der um einen Mechanismus der parlamentarischen Kontrolle zu ergänzen ist. Sinnvoll sind delegierte Rechtsakte, wenn der schnelle technische Fortschritt erwarten lässt, dass häufige Anpassungen der Regelungen an neue Gegebenheiten erforderlich werden.

Das FIfF fordert

⇒ Um die parlamentarische Kontrolle sicherzustellen, sind *delegierte Rechtsakte und Entscheidungen des Europäischen Datenschutzausschusses* in jedem Fall innerhalb einer angemessenen Frist (6 Monate) *vom Parlament zu bestätigen*.

⇒ Ein *Aufweichen von Regelungen* durch delegierte Rechtsakte muss effektiv *verhindert* werden.

⇒ Das *Demokratiedefizit* und die *Rechtsunsicherheit* müssen durch konkrete Regelungsinhalte *auf das absolute Mindestmaß reduziert* werden.

⇒ Es ist ein *enger Rahmen für die verbleibenden Befugnisse* vorzugeben, in dem sich delegierte Rechtsakte bewegen dürfen.

⇒ *Schutzziele* sind verbindlich vorzugeben, denen alle durch Rechtsakte vorgenommenen Konkretisierungen folgen müssen. Diese Schutzziele müssen den in der Fachwelt akzeptierten Schutzzielen des Datenschutzes und der Informationssicherheit folgen: Vertraulichkeit, Integrität, Verfügbarkeit sowie Transparenz, Zweckbindung und Intervenierbarkeit. Dabei ist sicherzustellen, dass *alle Prozesse bei Entwicklung und Nutzung der IT-Systeme* an diesen Schutzzielen ausgerichtet sind und sie erfüllen.

Begründung

Die in der Verordnung vorgesehenen Befugnisse der Kommission halten wir für zu weit gehend und höchst bedenklich. Sie würden zu einer großen Zahl an Detailregelungen führen, die der parlamentarischen Kontrolle entzogen sind. Die Kommission räumt sich dadurch das Recht ein, erhebliche Teile des Datenschutzrechts selbständig zu gestalten. Ist der Rahmen für delegierte Rechtsakte zu weit gefasst, wird damit die Substanz der Verordnung berührt.

In der Verordnung sind die praktischen Regelungen und konkreten Inhalte oft unklar, so dass eine erhebliche Rechtsunsicherheit für die betroffenen Stellen entsteht. Diese Rechtsunsicherheit gefährdet zum einen die effektive Durchsetzung von Bürgerrechten, zum anderen birgt sie wirtschaftliche Risiken, wenn die betroffenen Unternehmen keine Klarheit über die korrekte Anwendung und Umsetzung der Verordnung haben.

11. Für eine stärkere Unabhängigkeit der Aufsichtsbehörden und Datenschutzbeauftragten

Das FIfF begrüßt ausdrücklich die Festlegungen in Kapitel VI, Abschnitt 1 der Verordnung, die die Unabhängigkeit der Aufsichtsbehörden sicherstellen sollen. So heißt es in Art. 47, 1: „Die Aufsichtsbehörde handelt bei der Erfüllung der ihr übertragenen Aufgaben und Befugnisse völlig unabhängig."

Das FIfF begrüßt ebenfalls die Konkretisierungen im Änderungsvorschlag des Berichterstatters, dass die Angemessenheit unter Berücksichtigung der Bevölkerungszahl und des Umfangs der zu verarbeitenden personenbezogenen Daten zu bestimmen ist (Änderungsantrag 264). Und wir begrüßen die Klarstellung der Rechenschaftspflicht gegenüber den nationalen Parlamenten (Änderungsanträge 265, 266).

Diese Änderungen reichen aber nicht aus. Weitere Vorgaben sind zur Sicherstellung der Unabhängigkeit zu ergänzen.

Das FIfF fordert

⇒ Die Befugnis zu Ernennung der Mitglieder der Aufsichtsbehörden sollte (anders als in Art. 48, 1 formuliert) *ausschließlich* beim Parlament liegen Art. 48, 1 muss daher lauten: „Die Mitgliedsstaaten tragen dafür Sorge, dass die Mitglieder der Aufsichtsbehörde vom Parlament ernannt werden."

⇒ Genauere Vorgaben für die Finanzkontrolle sind nötig, die die Unabhängigkeit sicherstellen; zusätzlich müssen die *Aufsichtsbehörden finanziell so ausgestattet werden, dass sie ihren Aufgaben effektiv nachkommen können.*

⇒ Die Unabhängigkeit der *betrieblichen Datenschutzbeauftragten* sollte durch einen mindestens *einjährigen Kündigungsschutz* gestärkt werden. Deswegen fordern wir, Art. 35, 7 um folgenden Text zu ergänzen: „Ist ein Datenschutzbeauftragter zu bestellen, so ist die Kündigung des Arbeitsverhältnisses unzulässig, es sei denn, dass Tatsachen vorliegen, welche die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach der Abberufung als Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist."

Begründung

Die Aufsichtsbehörden und Datenschutzbeauftragten haben sich als Institutionen bewährt, die für die Einhaltung der Datenschutzvorschriften in Unternehmen und öffentlichen Einrichtungen sorgen und dabei beratend zur Seite stehen. In §4f (3) BDSG ist ein einjähriger Kündigungsschutz bereits festgelegt, er bietet sich als europaweite Regelung an.

Die Mitglieder der Aufsichtsbehörden sind als Vertreter der Interessen von Betroffenen zu betrachten. Als solche sollten sie von den gewählten Volksvertreterinnen und Volksvertretern bestimmt werden.

12. Für die Verpflichtung eines Datenschutzbeauftragten auch in kleineren Unternehmen

Das FIfF begrüßt ausdrücklich die Änderungsanträge 223 bis 225 des Berichterstatters, den Einsatz eines Datenschutzbeauftragten von der Anzahl der Betroffenen abhängig zu machen (Änderungsantrag 223) und die Profilerstellung (Änderungsantrag 224) sowie die Verarbeitung besonderer Kategorien von Daten (Änderungsantrag 225) explizit in den Katalog der Kerntätigkeiten aufzunehmen, die die Einsetzung eines Datenschutzbeauftragten erfordern.

Diese Änderungen reichen aber nicht aus.

Das FIfF fordert

⇒ die Bestellung eines Datenschutzbeauftragten in Art. 35, ergänzt um Änderungsantrag 223, mit der Vorgabe zu erweitern, dass die Bestellung verpflichtend ist, wenn „personenbezogene Daten … erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 10 Personen beschäftigt sind."

Begründung

Der Kommissionsentwurf sieht in Art. 35, 1 a) vor, dass ein betrieblicher Datenschutzbeauftragter durch Unternehmen erst ab einer Zahl von 250 Beschäftigten einzusetzen ist. Diese Zahl ist zu hoch, auch wenn die Situation von kleinen und mittleren Unternehmen berücksichtigt werden muss.

13. Zur Erhebung politischer Einstellungen durch Parteien

Erwägungsgrund 44 des Kommissionsentwurfs formuliert, dass politische Parteien Daten über die politische Einstellung von Personen sammeln dürfen. Dieses Recht gilt im Zusammenhang mit Wahlen aus Gründen des öffentlichen Interesses und ist an angemessene Garantien gebunden. Die Regelung wird auch im Vorschlag des Berichterstatters nicht geändert.

Das FIfF fordert

⇒ Die Ausnahme ist zu streichen.

Begründung

Das Recht, Daten über politische – genauso wie weltanschauliche – Einstellungen zu sammeln, halten wir für äußerst bedenklich. Es birgt das Risiko, dass diese *einmal angefallenen Daten* – auch zu einem späteren Zeitpunkt – *ausgewertet und zum Nachteil der Betroffenen verwendet* werden.

Zahlreiche Datenschutzvorfälle der vergangenen Zeit zeigen, dass eine effektive Sicherung von Daten nahezu unmöglich ist, so dass ein *Missbrauch niemals mit hinreichender Sicherheit ausgeschlossen* werden kann. Die dann drohenden Eingriffe in die Persönlichkeitsrechte der Betroffenen sind aus unserer Sicht nicht hinnehmbar.

14. Für die Regelung des Beschäftigten-Datenschutzes durch die Mitgliedstaaten

Das FIfF begrüßt ausdrücklich die Änderungen des Berichterstatters zu Erwägungsgrund 124.

Das FIfF fordert

⇒ Die Einschränkung der EU-Kommission, dass die Mitgliedstaaten dies nur in den Grenzen dieser Verordnung tun dürfen, muss entfallen.

Begründung

Wir unterstützen die Auffassung des Berichterstatters, dass „... der Beschäftigungssektor ... ein hochkomplexer Bereich [ist], der auf einzelstaatlicher Ebene detailliert geregelt ist. Daher sollten die Mitgliedstaaten die Möglichkeit haben, spezielle Gesetze zur detaillierten Regelung des Datenschutzes öffentlicher Einrichtungen in diesem Bereich zu erlassen oder beizubehalten."