2012/0011 (COD)

Vorschlag für

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)

(Text von Bedeutung für den EWR)

Anmerkungen und Änderungsvorschläge des Gesamtverbands der Deutschen Versicherungswirtschaft e. V.

Teil II: Artikel 22 bis 37

Stand: 31. August 2012

KAPITEL IV

FÜR DIE VERARBEITUNG VERANTWORTLICHER UND AUFTRAGSVERARBEITER

ABSCHNITT 1
ALLGEMEINE PFLICHTEN

Artikel 22 ***Pflichten des für die Verarbeitung Verantwortlichen***	EG 60.
1. Der für die Verarbeitung Verantwortliche stellt durch geeignete Strategien und Maßnahmen sicher, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden und er den Nachweis dafür erbringen kann.	
2. Die in Absatz 1 genannten Maßnahmen umfassen insbesondere	
a) die Dokumentation nach Maßgabe von Artikel 28;	Siehe Art. 28.
b) die Umsetzung der in Artikel 30 vorgesehenen Vorkehrungen für die Datensicherheit;	Siehe Art. 30.
c) die Durchführung einer Datenschutz-Folgenabschätzung nach Artikel 33;	Siehe Art. 33.
d) die Umsetzung der nach Artikel 34 Absätze 1 und 2 geltenden Anforderungen in Bezug auf die vorherige Genehmigung oder Zurateziehung der Aufsichtsbehörde;	Siehe Art. 34.
e) die Benennung eines Datenschutzbeauftragten gemäß Artikel 35 Absatz 1.	Siehe Art. 35.
3. Der für die Verarbeitung Verantwortliche setzt geeignete Verfahren zur Überprüfung der Wirksamkeit der in den Absätzen 1 und 2 genannten Maßnahmen ein. Die Überprüfung wird von unabhängigen internen oder externen Prüfern durchgeführt, wenn	

dies angemessen ist.	
4. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um etwaige weitere, in Absatz 2 nicht genannte Kriterien und Anforderungen für die in Absatz 1 genannten Maßnahmen, die Bedingungen für die in Absatz 3 genannten Überprüfungs- und Auditverfahren und die Kriterien für die in Absatz 3 angesprochene Angemessenheitsprüfung festzulegen und spezifische Maßnahmen für Kleinst-, Klein- und mittlere Unternehmen zu prüfen.	Eine nachträgliche und möglicherweise zeitlich verzögerte Festlegung der genannten Aspekte führt zu Rechtsunsicherheit für alle Unternehmen. Die Sachverhalte sind in der Verordnung bereits ausreichend geregelt. **GDV-Vorschlag:** **Art. 22 Abs. 4 wird gestrichen.**
Artikel 23 ***Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen***	EG 61.
1. Der für die Verarbeitung Verantwortliche führt unter Berücksichtigung des Stands der Technik und der Implementierungskosten sowohl zum Zeitpunkt der Festlegung der Verarbeitungsmittel als auch zum Zeitpunkt der Verarbeitung technische und organisatorische Maßnahmen und Verfahren durch, durch die sichergestellt wird, dass die Verarbeitung den Anforderungen dieser Verordnung genügt und die Rechte der betroffenen Person gewahrt werden.	
2. Der für die Verarbeitung Verantwortliche setzt Verfahren ein, die sicherstellen, dass grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, die für die spezifischen Zwecke der Verarbeitung benötigt werden, und dass vor allem nicht mehr personenbezogene Daten zusammengetragen oder vorgehalten werden als für diese Zwecke unbedingt nötig ist und diese Daten auch nicht länger als für diese Zwecke unbedingt erforderlich gespeichert werden. Die Verfahren müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.	Die Anzahl der Personen, die in einem Unternehmen Zugang zu einem Datum haben, bringt nicht allein Risiken für das Datensubjekt mit sich. Es kommt dabei auch darauf an, welcher Personenkreis mit welchen Aufgaben und Verpflichtungen Zugang hat. Bei einem lang laufenden Versicherungsvertrag (zum Beispiel über 50 Jahre bei einem Rentenversicherungsvertrag) ist die Zahl der involvierten Mitarbeiter nicht à priori zu begrenzen, der Personenkreis jedoch schon. **GDV-Vorschlag:** Art. 23 Abs. 2 Satz 2 wird wie folgt gefasst: „Die Verfahren müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nicht **einem unbestimmten Personenkreis** zugänglich gemacht werden.“
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um etwaige weitere Kriterien und Anforderungen in Bezug auf die in den Absätzen 1 und 2 genannten Maßnahmen und Verfahren festzulegen, speziell was die Anforderungen an den Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen für ganze Sektoren und bestimmte Erzeugnisse und Dienstleistungen betrifft.	Nach Art. 290 AEUV soll in delegierten Rechtsakten kein wesentlicher Aspekt einer gesetzlichen Regelung bestimmt werden. Entsprechend diesem Grundsatz geht die Regulierung der Anforderungen an „ganze Sektoren und bestimmte Erzeugnisse und Dienstleistungen“ zu weit. Die Regulierung dieser Aspekte sollte den Mitgliedstaaten überlassen werden. **GDV-Vorschlag:** **Art. 23 Abs. 3 wird gestrichen.**
4. Die Kommission kann technische Standards für die in den Absätzen 1 und 2 genannten Anforderungen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.	Der Nutzen der Festlegung technischer Standards durch die Kommission ist fraglich. Auf diese Weise kann kaum flexibel auf schnelle Änderungen technische Standards und unterschiedliche Anforderungen in verschiedenen Bereichen reagiert werden. **GDV-Vorschlag:** **Art. 23 Abs. 4 wird gestrichen.**

Artikel 24 ***Gemeinsam für die Verarbeitung Verantwortliche***	EG 62.
In allen Fällen, in denen ein für die Verarbeitung Verantwortlicher die Zwecke, Bedingungen und Mittel der Verarbeitung personenbezogener Daten gemeinsam mit anderen Personen festlegt, vereinbaren diese gemeinsam für die Verarbeitung Verantwortlichen, wer von ihnen welche ihnen gemäß dieser Verordnung obliegenden Aufgaben erfüllt, insbesondere was die Verfahren und Mechanismen betrifft, die den betroffenen Person die Wahrnehmung ihrer Rechte ermöglichen.	Eine gesetzliche Grundlage für die arbeitsteilige Datenverarbeitung ist (auch wenn Gesundheitsdaten betroffen sind!), dringend erforderlich. Es muss z.B. in Versicherungskonzernen möglich sein, die Leistungs- und Risikoprüfungen in der Konzernmuttergesellschaft oder in spezialisierten Konzerntöchtern vorzunehmen. Eine konzernübergreifende Datenverarbeitung entspricht längst der Praxis in Unternehmensgruppen und ist gerade für die Versicherungswirtschaft aufgrund des für sie geltenden Spartentrennungsprinzips immens wichtig. Auch muss es möglich sein, für einzelne Abgaben spezialisierte Externe einzuschalten. Ohne Dienstleister, wie z. B. ärztliche Gutachter, Gesundheitsdienste und Rückversicherer, ist das Versicherungsgeschäft nicht denkbar (vgl. Anmerkungen zu Art. 9 und 81). Art. 24 ist für die Regelung der gemeinsamen Datenverarbeitung nicht hilfreich, weil er keine eindeutige Ermächtigungsgrundlage für eine Datenweitergabe von einer verantwortlichen Stelle an die andere schafft. Sobald eine gesamte Aufgabe übertragen wird, liegt nach Auffassung vieler Datenschutzbehörden keine Auftragsdatenverarbeitung vor, sodass Art. 26 nicht eingreift. **GDV-Vorschlag:** In Art. 24 sollte ausdrücklich klargestellt werden, dass die Stellen im Hinblick auf die für die gemeinsame Datenverarbeitung erforderlichen Datenübermittlungen wie eine verantwortliche Stelle behandelt werden.
Artikel 25 ***Vertreter von nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen***	EG 63, 64.
1. Jeder für die Verarbeitung Verantwortliche, der sich in der in Artikel 3 Absatz 2 beschriebenen Situation befindet, benennt einen Vertreter in der Union.	
2. Diese Pflicht gilt nicht für	
a) für die Verarbeitung Verantwortliche, die in einem Drittland niedergelassen sind, das laut Beschluss der Kommission einen angemessenen Schutz im Sinne von Artikel 41 bietet; oder	
b) Unternehmen, die weniger als 250 Mitarbeiter beschäftigen; oder	
c) Behörden oder öffentliche Einrichtungen; oder	
d) für die Verarbeitung Verantwortliche, die in der Union ansässigen betroffenen Personen nur gelegentlich Waren oder Dienstleistungen anbieten.	
3. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die betroffenen Personen, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird, ansässig sind.	

4. Die Benennung eines Vertreters durch den für die Verarbeitung Verantwortlichen erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den für die Verarbeitung Verantwortlichen.	
Artikel 26 ***Auftragsverarbeiter***	EG 65, 66.
1. Der für die Verarbeitung Verantwortliche wählt für alle in seinem Auftrag durchzuführenden Verarbeitungsvorgänge einen Auftragsverarbeiter aus, der hinreichende Garantien dafür bietet, dass die betreffenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und dass der Schutz der Rechte der betroffenen Person durch geeignete technische Sicherheitsvorkehrungen und organisatorische Maßnahmen für die vorzunehmende Verarbeitung sichergestellt wird; zudem sorgt er dafür, dass diese Maßnahmen eingehalten werden.	Die Reichweite des Begriffs der Auftragsdatenverarbeitung ist sehr unsicher. Die deutschen Datenschutzbehörden bevorzugen z.B. eine sehr enge Auslegung. Sie gehen davon aus, dass die entsprechende Bestimmung des § 11 BDSG nur eine Privilegierung schaffen kann, wenn untergeordnete Hilfstätigkeiten übertagen werden. Nur dann könne ein Weisungsrecht im Hinblick auf die Datenverarbeitung bestehen. Damit sind die in der Praxis wichtigen Übertragungen von Funktionen zur selbständigen Bearbeitung (z.B. Risiko- und Leistungsbearbeitung in der Versicherungswirtschaft) nicht erfasst. Diese Trennung zum Schutz personenbezogener Daten ist nicht erforderlich, solange klare Grenzen gezogen werden, die sicherstellen, dass die Daten zweckentsprechend verwendet werden. Es gibt in der Praxis außerdem erhebliche Abgrenzungsschwierigkeiten zwischen den Fällen, in denen eine Auftragsdatenverarbeitung anzunehmen ist oder eine Datenübermittlung vorliegt. **GDV-Vorschlag:** Es sollte klargestellt werden, dass Art. 26 nicht auf die Übertragung untergeordneter Tätigkeiten beschränkt ist, sondern auch eingreift, wenn Funktionen zur selbständigen Bearbeitung übertragen werden. Alternativ ist dringend eine Rechtsgrundlage für diese Fälle in Art. 24 zu schaffen (dazu oben).
2. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem insbesondere vorgesehen ist, dass der Auftragsverarbeiter	
a) nur auf Weisung des für die Verarbeitung Verantwortlichen tätig wird, insbesondere in Fällen, in denen eine Übermittlung der personenbezogenen Daten nicht zulässig ist;	
b) ausschließlich Mitarbeiter beschäftigt, die sich zur Vertraulichkeit verpflichtet haben oder der gesetzlichen Verschwiegenheitspflicht unterliegen;	
c) alle in Artikel 30 genannten erforderlichen Maßnahmen ergreift;	
d) die Dienste eines weiteren Auftragsverarbeiters nur mit vorheriger Zustimmung des für die Verarbeitung Verantwortlichen in Anspruch nehmen darf;	
e) soweit es verarbeitungsbedingt möglich ist, in Absprache mit dem für die Verarbeitung Verantwortlichen die notwendigen technischen und organisatorischen Voraussetzungen dafür schafft, dass der für die Verarbeitung Verantwortliche seine Pflicht erfül-	

len kann, Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;	
f) den Auftragsverarbeiter bei der Einhaltung der in den Artikeln 30 bis 34 genannten Pflichten unterstützt;	Hier kann nur der ‚für die Verarbeitung Verantwortliche' gemeint sein. Dies muss in der deutschen Sprachfassung geändert werden.
g) nach Abschluss der Verarbeitung dem für die Verarbeitung Verantwortlichen sämtliche Ergebnisse aushändigt und die personenbezogenen Daten auf keine andere Weise weiterverarbeitet;	
h) dem für die Verarbeitung Verantwortlichen und der Aufsichtsbehörde alle erforderlichen Informationen für die Kontrolle der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt.	Bei der Auftragsdatenverarbeitung trägt nicht der Auftragsdatenverarbeiter die Verantwortung gegenüber der Aufsichtsbehörde. Ansprechpartner ist der für die Verarbeitung Verantwortliche. Er sollte daher in erster Linie die Informationen erhalten. Die Informationspflicht des Auftragsdatenverarbeiters an die Aufsichtsbehörde sollte ausschließlich auf Informationen zu den technischen und organisatorischen Maßnahmen begrenzt werden. **GDV-Vorschlag:** Art. 26 Abs. 2 h wird wie folgt gefasst: „dem für die Verarbeitung Verantwortlichen alle erforderlichen Informationen für die Kontrolle der Einhaltung der in diesem Artikel niedergelegten Pflichten **und der Aufsichtsbehörde Informationen über die ergriffenen technischen und organisatorischen Maßnahmen** zur Verfügung stellt."
3. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter dokumentieren die Anweisungen des für die Verarbeitung Verantwortlichen und die in Absatz 2 aufgeführten Pflichten des Auftragsverarbeiters.	
4. Jeder Auftragsverarbeiter, der personenbezogene Daten auf eine andere als die ihm von dem für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet, gilt für diese Verarbeitung als für die Verarbeitung Verantwortlicher und unterliegt folglich den Bestimmungen des Artikels 24 für gemeinsam für die Verarbeitung Verantwortliche.	Diese Formulierung von Art. 26 Abs. 4 beachtet nicht, dass im beschriebenen Fall Art. 24 nicht sinnvoll gelten kann. Der eigentliche Auftragsverarbeiter hat die Daten anders als mit dem für die Verarbeitung Verantwortlichen verabredet verarbeitet, d.h. es besteht kein Einverständnis und keine Einigung über die Art der Verarbeitung oder eine gemeinsame Verantwortung der Verarbeitung. Gilt aber doch Art. 24 uneingeschränkt, so könnte es dazu kommen, dass der eigentlich für die Verarbeitung Verantwortliche für die Auswirkungen von Datenpannen haften muss, welche außerhalb der von ihm festgelegten Parameter hervorgerufen wurden. **GDV-Vorschlag:** Art. 26 Abs. 4 wird wie folgt gefasst: „Jeder Auftragsverarbeiter, der personenbezogene Daten auf eine andere als die ihm von dem für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet, gilt für diese Verarbeitung als für die Verarbeitung **Verantwortlicher.**"
5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die Verantwortlichkeiten, Pflichten und Aufgaben des	Eine weitere Konkretisierung der Kriterien und Anforderungen durch delegierte Rechtsakte ist nicht erforderlich. Die Bestimmung der Bedingungen für die Verarbeitung personenbezogener Daten in Unter-

Auftragsverarbeiters in Übereinstimmung mit Absatz 1 festzulegen sowie die Bedingungen, durch die die Verarbeitung personenbezogener Daten in Unternehmensgruppen speziell zu Kontroll- und Berichterstattungszwecken vereinfacht werden kann.	nehmensgruppen ist eine wesentliche Regelung, die nach Art. 290 AEUV nicht delegierten Rechtsakten überlassen bleiben darf. Insbesondere die Versicherungswirtschaft ist aufgrund des für sie geltenden Spartentrennungsgrundsatzes auf eine sichere Grundlage für die Datenverarbeitung im Konzern angewiesen (dazu Anmerkungen zu Art. 9 und Art. 24). Insoweit erscheint der Verordnungsentwurf wenig stringent. Einerseits scheint er eine solche in Art. 4 Abs. 5, 24, 26 Abs. 5 vorauszusetzen. Andererseits soll die Kommission solche Verarbeitungen (nur zum Zweck der Kontrolle und Berichterstattung) „vereinfachen“ können. **GDV-Vorschlag:** **Art. 26 Abs. 5 wird gestrichen.**
Artikel 27 ***Verarbeitung unter der Aufsicht des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters***	
Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind und Zugang zu personenbezogenen Daten haben, sowie der Auftragsverarbeiter selbst dürfen personenbezogene Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten, sofern sie keinen anders lautenden, aus dem Unionsrecht oder dem mitgliedstaatlichen Recht erwachsenden Pflichten unterliegen.	
Artikel 28 ***Dokumentation***	
1. Alle für die Verarbeitung Verantwortlichen, alle Auftragsverarbeiter sowie etwaige Vertreter von für die Verarbeitung Verantwortlichen dokumentieren die ihrer Zuständigkeit unterliegenden Verarbeitungsvorgänge.	
2. Die Dokumentation enthält mindestens folgende Informationen:	
a) Name und Kontaktdaten des für die Verarbeitung Verantwortlichen (oder etwaiger gemeinsam für die Verarbeitung Verantwortlicher) oder des Auftragsverarbeiters sowie eines etwaigen Vertreters;	
b) Name und Kontaktdaten eines etwaigen Datenschutzbeauftragten;	
c) Angaben über die Zwecke der Verarbeitung sowie – falls sich die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f gründet – über die von dem für die Verarbeitung Verantwortlichen verfolgten legitimen Interessen;	
d) eine Beschreibung der Kategorien von betroffenen Personen und der Kategorien der sich auf diese beziehenden personenbezogenen Daten;	
e) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten einschließlich der für die Verarbeitung Verantwortlichen, denen personenbezogene Daten aus dem von diesen verfolgtem legitimen Interesse mitgeteilt werden;	

f) gegebenenfalls Angaben über etwaige Datenübermittlungen in Drittländer oder an internationale Organisationen einschließlich deren Namen sowie bei den in Artikel 44 Absatz 1 Buchstabe h genannten Datenübermittlungen ein Beleg dafür, dass geeignete Sicherheitsgarantien vorgesehen wurden;	
g) eine allgemeine Angabe der Fristen für die Löschung der verschiedenen Datenkategorien	
h) eine Beschreibung der in Artikel 22 Absatz 3 genannten Verfahren.	
3. Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Vertreter des für die Verarbeitung Verantwortlichen stellen die Dokumentation der Aufsichtsbehörde auf Anforderung zur Verfügung.	
4. Die in den Absätzen 1 und 2 genannten Anforderungen gelten nicht für folgende für die Verarbeitung Verantwortliche und Auftragsverarbeiter:	
a) natürliche Personen, die personenbezogene Daten ohne eigenwirtschaftliches Interesse verarbeiten; oder	
b) Unternehmen oder Organisationen mit weniger als 250 Beschäftigten, die personenbezogene Daten nur als Nebentätigkeit zusätzlich zu ihren Haupttätigkeiten verarbeiten.	
5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in Absatz 1 genannte Dokumentation festzulegen, so dass insbesondere den Verantwortlichkeiten des für die Verarbeitung Verantwortlichen, des Auftragsverarbeiters sowie des etwaigen Vertreters des für die Verarbeitung Verantwortlichen Rechnung getragen wird.	Die Kriterien und Anforderungen für die nach Absatz 1 zu erstellende Dokumentation sind bereits in Absatz 2 enthalten und ausreichend. **GDV-Vorschlag:** **Art. 28 Abs. 5 wird gestrichen.**
6. Die Kommission kann Standardvorlagen für die in Absatz 1 genannte Dokumentation festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren angenommen.	Während die sicherlich hinter diesem Absatz stehende Intention der EU-weiten Harmonisierung positiv ist, so ist es fraglich, ob durch Standardvorlagen ein praktischer Nutzen erreicht werden kann. Diese könnten z.B. den unterschiedlichen Realitäten von Unternehmen widersprechen (z.B. Online- vs. Offline-Tätigkeit). **GDV-Vorschlag:** **Art. 28 Abs. 6 wird gestrichen.**
Artikel 29 ***Zusammenarbeit mit der Aufsichtsbehörde***	
1. Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Vertreter des für die Verarbeitung Verantwortlichen arbeiten der Aufsichtsbehörde auf Verlangen zu, um ihr die Erfüllung ihrer Pflichten zu erleichtern, indem sie dieser insbesondere die in Artikel 53 Absatz 2 Buchstabe a genannten Informationen übermitteln und ihr den in Artikel 53 Absatz 2 Buchstabe b genannten Zugang gewähren.	Soweit es um den Inhalt einer Datenverarbeitung geht, muss sich die Aufsichtsbehörde an den für die Verarbeitung Verantwortlichen wenden. Der Auftragsdatenverarbeiter sollte nur die Erfüllung der technischen und organisatorischen Anforderungen nachweisen müssen (vgl. auch Anmerkungen zu Art. 26).

2. Auf von der Aufsichtsbehörde im Rahmen der Ausübung ihrer Befugnisse erteilte Anordnungen gemäß Artikel 53 Absatz 2 antworten der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter der Aufsichtsbehörde binnen einer von der Aufsichtsbehörde zu setzenden angemessenen Frist. Die Antwort muss auch eine Beschreibung der im Anschluss an die Bemerkungen der Aufsichtsbehörde getroffenen Maßnahmen und der damit erzielten Ergebnisse beinhalten.	

ABSCHNITT 2
DATENSICHERHEIT

Artikel 30 ***Sicherheit der Verarbeitung***	
1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter Berücksichtigung des Stands der Technik und der Implementierungskosten technische und organisatorische Maßnahmen, die geeignet sind, ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.	
2. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen im Anschluss an eine Risikobewertung die in Absatz 1 genannten Maßnahmen zum Schutz personenbezogener Daten vor unbeabsichtigter oder widerrechtlichen Zerstörung oder vor unbeabsichtigtem Verlust sowie zur Vermeidung jedweder unrechtmäßigen Verarbeitung, insbesondere jeder unbefugten Offenlegung, Verbreitung beziehungsweise Einsichtnahme oder Veränderung.	
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Bedingungen für die in den Absätzen 1 und 2 genannten technischen und organisatorischen Maßnahmen festzulegen und den aktuellen Stand der Technik für bestimmte Sektoren und Datenverarbeitungssituationen zu bestimmen, wobei sie die technologische Entwicklung sowie Lösungen für einen Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen berücksichtigt, sofern nicht Artikel 4 gilt.	Der aktuelle Stand der Technik ändert sich ständig. Es kann nicht erwartet werden, dass die Kommission ihn so engmaschig verfolgt, dass jede Neuerung abgedeckt werden kann. Zudem würde die Kommission auf Jahre hinaus ständig zum selben Sachverhalt neue delegierte Rechtsakte auflegen oder alte überarbeiten müssen. Dies steht nicht im Verhältnis zum davon erhofften Effekt. **GDV-Vorschlag:** **Art. 30 Abs. 3 wird gestrichen.**
4. Die Kommission kann erforderlichenfalls Durchführungsbestimmungen zu einer situationsabhängigen Konkretisierung der in den Absätzen 1 und 2 genannten Anforderungen erlassen, um insbesondere	In besonderen Situationen auf der Basis datenschutzrechtlicher Bestimmungen konkrete Maßnahmen zu ergreifen, ist Aufgabe der Datenschutzaufsichtsbehörden. Durchführungsbestimmungen werden in aller Regel nicht erforderlich sein. **GDV-Vorschlag:** **Art. 30 Abs. 4 wird gestrichen.**
a) jedweden unbefugten Zugriff auf personenbezogene Daten zu verhindern;	
b) jedwede unbefugte Einsichtnahme in personenbezogene Daten sowie jedwede unbefugte Offenle-	

gung, Kopie, Änderung, Löschung oder Entfernung von personenbezogenen Daten zu verhindern;	
c) sicherzustellen, dass die Rechtmäßigkeit der Verarbeitungsvorgänge überprüft wird.	
Die genannten Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren angenommen.	
Artikel 31 ***Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde***	EG 67 - 69.
1. Bei einer Verletzung des Schutzes personenbezogener Daten benachrichtigt der für die Verarbeitung Verantwortliche die Aufsichtsbehörde ohne unangemessene Verzögerung und nach Möglichkeit binnen 24 Stunden nach Feststellung der Verletzung. Falls die Meldung an die Aufsichtsbehörde nicht binnen 24 Stunden erfolgt, ist dieser eine Begründung beizufügen.	Nach Art. 31 Abs. 1 muss jede Datenpanne an die Aufsichtsbehörde gemeldet werden. Es wird dabei nicht in Betracht gezogen, ob die Daten ihrer Art nach besonders schutzwürdig sind und welche Schwere und Tragweite der Vorfall für die Betroffenen hat. Ein so weit gefasster Anwendungsbereich lässt eine Meldeflut bei den Aufsichtsbehörden und eine Abstumpfung der immer wieder auch in nichtigen Fällen benachrichtigten Betroffenen befürchten. Die angedachte Frist für die Meldung einer Datenpanne innerhalb von 24 Stunden wird oft nicht ausreichen, vollständig zu klären, ob überhaupt eine Datenpanne vorliegt und welches Ausmaß sie hat. Abhängig von der Schwere der Datenpanne, wie auch von möglicherweise beteiligten Schwesterunternehmen in einem Konzern oder Auftragsdatenverarbeitern, müssten eventuell weitere interne Verantwortliche oder auch externe Experten hinzugezogen werden. Es wäre daher besser, hier nur eine Meldung ‚ohne unangemessene Verzögerung' zu fordern. **GDV-Vorschlag:** Art. 31 sollte so eingeschränkt werden, dass • nur besonders schutzwürdige Daten erfasst sind, • nur die unrechtmäßige Übermittlung oder sonstige unrechtmäßige Kenntniserlangung erfasst sind und, • schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen müssen. Als Vorbild kann der im Jahr 2009 in das deutsche Bundesdatenschutzgesetz eingefügte § 42a BDSG dienen. Die Meldung sollte ohne unangemessene Verzögerung erfolgen müssen.
2. In Übereinstimmung mit Artikel 26 Absatz 2 Buchstabe f alarmiert und informiert der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen unmittelbar nach Feststellung einer Verletzung des Schutzes personenbezogener Daten.	
3. Die in Absatz 1 genannte Benachrichtigung enthält mindestens folgende Informationen:	
a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Datenkategorien und der Zahl der	

betroffenen Datensätze;	
b) Name und Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen;	
c) Empfehlungen für Maßnahmen zur Eindämmung etwaiger negativer Auswirkungen der Verletzung des Schutzes personenbezogener Daten;	
d) eine Beschreibung der Folgen der Verletzung des Schutzes personenbezogener Daten;	
e) eine Beschreibung der vom für die Verarbeitung Verantwortlichen vorgeschlagenen oder ergriffenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten.	
4. Der für die Verarbeitung Verantwortliche dokumentiert etwaige Verletzungen des Schutzes personenbezogener Daten unter Beschreibung aller im Zusammenhang mit der Verletzung stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Die Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen. Die Dokumentation enthält nur die zu diesem Zweck erforderlichen Informationen.	Die hier geforderte umfassende Dokumentation dürfte - abgesehen von einem enormen bürokratischen Aufwand - wirkungslos sein. Effizienter ist es, die wesentlichen Fakten zu dokumentieren. **GDV-Vorschlag:** Art. 31 Abs. 4 wird wie folgt gefasst: „Der für die Verarbeitung Verantwortliche dokumentiert etwaige Verletzungen des Schutzes personenbezogener Daten unter **Benennung der wesentlichen** im Zusammenhang mit der Verletzung stehenden Fakten […].“
5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen in Bezug auf die Feststellung der in den Absätzen 1 und 2 genannten Verletzungen des Schutzes personenbezogener Daten festzulegen sowie die konkreten Umstände, unter denen der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten zu melden haben.	Insbesondere die Ermächtigung der Kommission zur weitergehenden Definition der Verletzung des Schutzes personenbezogener Daten erscheint zu weitgehend und birgt enorme Rechtsunsicherheit in sich. Stattdessen sollte die Definition bereits in Art. 4 Abs. 9 stärker eingeengt werden, vgl. dort. **GDV-Vorschlag:** **Art. 31 Abs. 5 wird gestrichen.**
6. Die Kommission kann das Standardformat für derartige Meldungen an die Aufsichtsbehörde, die Verfahrensvorschriften für die vorgeschriebene Meldung sowie Form und Modalitäten der in Absatz 4 genannten Dokumentation einschließlich der Fristen für die Löschung der darin enthaltenen Informationen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.	Während die sicherlich hinter diesem Absatz stehende Intention der EU-weiten Harmonisierung positiv ist, so ist es fraglich, ob durch Standardvorlagen ein praktischer Nutzen erreicht werden kann. Diese könnten z.B. den unterschiedlichen Realitäten von Unternehmen widersprechen (z.B. Online- vs. Offline-Tätigkeit). **GDV-Vorschlag:** **Art. 31 Abs. 6 wird gestrichen.**
Artikel 32 ***Benachrichtigung der betroffenen Person von einer Verletzung des Schutzes ihrer personenbezogenen Daten***	
1. Der für die Verarbeitung Verantwortliche benachrichtigt im Anschluss an die Meldung nach Artikel 31 die betroffene Person ohne unangemessene Verzögerung von der Verletzung des Schutzes personenbezogener Daten, wenn die Wahrscheinlichkeit besteht, dass der Schutz der personenbezogenen Daten oder der Privatsphäre der betroffenen Person	Damit die Benachrichtigung ihre beabsichtigte Wirkung erzielt, muss eine Abstumpfung der Betroffenen durch Meldungen in trivialen Fällen vermieden werden. **GDV-Vorschlag:** Art. 32 Abs. 1 sollte wie für Art. 31 vorgeschlagen

durch eine festgestellte Verletzung des Schutzes personenbezogener Daten beeinträchtigt wird.	eingeschränkt werden.
2. Die in Absatz 1 genannte Benachrichtigung der betroffenen Person umfasst mindestens die in Artikel 31 Absatz 3 Buchstaben b und c genannten Informationen und Empfehlungen.	
3. Die Benachrichtigung der betroffenen Person über die Verletzung des Schutzes personenbezogener Daten ist nicht erforderlich, wenn der für die Verarbeitung Verantwortliche zur Zufriedenheit der Aufsichtsbehörde nachweist, dass er geeignete technische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden. Durch diese technischen Sicherheitsvorkehrungen sind die betreffenden Daten für alle Personen zu verschlüsseln, die nicht zum Zugriff auf die Daten befugt sind.	
4. Unbeschadet der dem für die Verarbeitung Verantwortlichen obliegenden Pflicht, der betroffenen Person die Verletzung des Schutzes personenbezogener Daten mitzuteilen, kann die Aufsichtsbehörde, falls der für die Verarbeitung Verantwortliche die betroffene Person noch nicht in Kenntnis gesetzt hat, nach Prüfung der zu erwartenden negativen Auswirkungen der Verletzung den für die Verarbeitung Verantwortlichen auffordern, dies zu tun.	
5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen in Bezug auf die Umstände festzulegen, unter denen sich eine Verletzung des Schutzes personenbezogener Daten negativ auf die in Absatz 1 genannten personenbezogenen Daten auswirken kann.	Die Definition von Umständen, „unter denen sich eine Verletzung des Schutzes personenbezogener Daten negativ auf die in Absatz 1 genannten personenbezogenen Daten auswirken kann“ sollte bereits in der Verordnung, am besten in Art. 31 Abs. 1 und 32 Abs. 1 (vgl. GDV-Vorschlag) oder in Art. 4 Abs. 9, geschehen. Eine Bestimmung durch delegierte Rechtsakte bietet den Unternehmen keine ausreichende Rechtssicherheit. **GDV-Vorschlag:** **Art. 32 Abs. 5 wird gestrichen.**
6. Die Kommission kann das Format für die in Absatz 1 genannte Mitteilung an die betroffene Person und die für die Mitteilung geltenden Verfahrensvorschriften festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.	Es ist fraglich, ob durch Standardvorlagen ein praktischer Nutzen erreicht werden kann. Diese könnten z.B. den unterschiedlichen Realitäten von Unternehmen widersprechen (z.B. Online- vs. Offline-Tätigkeit). **GDV-Vorschlag:** **Art. 32 Abs. 6 wird gestrichen.**

ABSCHNITT 3
DATENSCHUTZ-FOLGENABSCHÄTZUNG UND VORHERIGE GENEHMIGUNG

Artikel 33 ***Datenschutz-Folgenabschätzung***	EG 70 - 74.
1. Bei Verarbeitungsvorgängen, die aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener	Angesichts der Vielzahl von Verpflichtungen, die bereits bestehen, ist eine zusätzliche Verpflichtung zur Datenschutzfolgenabschätzung nach Art. 33 nicht

Personen bergen, führt der für die Verarbeitung Verantwortliche oder der in seinem Auftrag handelnde Auftragsverarbeiter vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.	nachvollziehbar. Zudem ist der Anwendungsbereich der Norm nicht eindeutig. So stellt sich die Frage, wann ein Verarbeitungsvorgang „konkrete Risiken für die Rechte und Freiheiten betroffener Personen“ birgt. Auch ist nicht klar, welchen Inhalt und Umfang die Folgenabschätzung haben soll (nach Art. 33 Abs. 6 der Kommission überlassen). Da die Auswirkungen einer Datenverarbeitung für die Betroffenen ohnehin im Rahmen der anderen Anforderungen, wie z. B. des Art. 23, beachtet werden müssen, ist Art. 33 entbehrlich. **GDV-Vorschlag:** Art. 33 sollte möglichst gestrichen werden. Es sollte geprüft werden, ob die Vorabkontrolle durch einen Datenschutzbeauftragten nicht eine bessere Alternative ist. Zumindest bedarf die Norm dringend einer grundlegenden Überarbeitung.
2. Die in Absatz 1 genannten Risiken bestehen insbesondere bei folgenden Verarbeitungsvorgängen:	Die Norm erfasst bei weiter Auslegung nahezu alle Datenverarbeitungen in der Versicherungswirtschaft. Die Lebens-, Kranken- und Unfallversicherung fällt schon darunter, weil die Verarbeitung von Gesundheitsdaten notwendig ist. Bei weiter Auslegung des Begriffs der Profilbildung könnten zudem auch Tarifeinstufungen eine Folgenabschätzung erforderlich machen. Sie würde damit zu enormem bürokratischem Aufwand für die Branche führen. Dabei ist mit der Verarbeitung – auch von Gesundheitsdaten – zu Versicherungszwecken in aller Regel keine besondere Gefährdung der Betroffenen verbunden, weil lediglich ihre Verträge durchgeführt oder gesetzlichen Ansprüche erfüllt werden. Welche Daten, etwa zur Risikoprüfung oder Leistungsbearbeitung, verarbeitet werden, ist dem Kunden oder Antragsteller in aller Regel bereits aus den Antragsfragen bzw. seinen eingereichten Unterlagen bekannt. Die Daten werden nur zu Versicherungszwecken verwendet. **GDV-Vorschlag:** Die Fallgruppen bedürfen daher dringend einer grundlegenden Überarbeitung, um die Sachverhalte zu erfassen, die im Hinblick auf Datenschutz und Datensicherheit wirklich mit hohen Risiken behaftet sind.
a) systematische und umfassende Auswertung persönlicher Aspekte einer natürlichen Person, beispielsweise zwecks Analyse ihrer wirtschaftlichen Lage, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens oder zwecks diesbezüglicher Voraussagen, die sich auf eine automatisierte Verarbeitung von Daten gründet und ihrerseits als Grundlage für Maßnahmen dient, welche Rechtswirkung gegenüber der betroffenen Person entfalten oder erhebliche Auswirkungen für diese mit sich bringen;	Siehe Anmerkungen unter 2.
b) Verarbeitung von Daten über das Sexualleben, den Gesundheitszustand, die Rasse oder die ethnische Herkunft oder für die Erbringung von Gesundheits-	Siehe Anmerkungen unter 2.

diensten, für epidemiologische Studien oder für Erhebungen über Geisteskrankheiten oder ansteckende Krankheiten, wenn die betreffenden Daten in großem Umfang im Hinblick auf Maßnahmen oder Entscheidungen verarbeitet werden, welche sich auf spezifische Einzelpersonen beziehen sollen;	
c) weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels Videoüberwachung;	
d) Verarbeitung personenbezogener Daten aus umfangreichen Dateien, die Daten über Kinder, genetische Daten oder biometrische Daten enthalten;	Siehe Anmerkungen unter 2. Die Dateien der Versicherer enthalten (auch) Daten über Kinder, die von ihren Eltern vertreten werden. Sie können auch genetische Daten enthalten, wenn z.B. ein Arzt eine genetische Analyse zur Diagnose einer Erkrankung benutzt hat. Diese Daten werden wie andere Gesundheitsdaten auch behandelt. Insofern bestehen keine besonderen Gefahren, die eine Folgenabschätzung rechtfertigen. **GDV-Vorschlag:** Art. 33 Abs. 2 d sollte zumindest wie folgt formuliert werden: „Verarbeitung personenbezogener Daten aus umfangreichen Dateien, die **ausschließlich oder in großem Umfang** Daten über Kinder, genetische Daten oder biometrische Daten enthalten
e) Sonstige Verarbeitungsvorgänge, bei denen gemäß Artikel 34 Absatz 2 Buchstabe b vorab die Aufsichtsbehörde zu Rate zu ziehen ist.	Die Bestimmung ist zu vage, weil die Bestimmung der Notwendigkeit einer Datenschutz-Folgenabschätzung damit den Datenschutzaufsichtsbehörden überlassen wird. **GDV-Vorschlag:** **Art. 33 Abs. 2 e wird gestrichen.**
3. Die Folgenabschätzung trägt den Rechten und den berechtigten Interessen der von Datenverarbeitung betroffenen Personen und sonstiger Betroffener Rechnung; sie enthält zumindest eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken sowie der geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden.	
4. Der für die Verarbeitung Verantwortliche holt die Meinung der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.	Die Einholung der Einschätzung der Betroffenen oder ihrer Repräsentanten (wie etwa des vzbv) gefährdet nicht nur Geschäftsgeheimnisse, sondern stellt auch einen unverhältnismäßigen Eingriff in die unternehmerische Freiheit dar. Soweit erforderlich kann nur eine objektive Prüfung durch staatliche Datenschutzaufsichtsbehörden in Betracht kommen. **GDV-Vorschlag:** **Art. 33 Abs. 4 wird gestrichen.**
5. Falls es sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde oder um eine öffentliche Einrichtung handelt und die Verarbeitung aufgrund	Die vorgeschlagene Formulierung lässt den Mitgliedstaaten einen sehr weiten Spielraum. Das könnte z.B. dazu führen, dass öffentliche Versicherer keine Fol-

einer im Unionsrecht festgelegten rechtlichen Verpflichtung nach Artikel 6 Absatz 1 Buchstabe c erfolgt, welche Vorschriften und Verfahren für die betreffenden Verarbeitungsvorgänge vorsieht, gelten die Absätze 1 bis 5 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.	genabschätzung durchführen müssen und private Versicherer dies tun müssen. **GDV-Vorschlag:** **Art. 33. Abs. 5 wird gestrichen.**
6. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Bedingungen für Verarbeitungsvorgänge, die mit den in den Absätzen 1 und 2 genannten Risiken behaftet sein können, sowie die Anforderungen an die in Absatz 3 genannte Folgenabschätzung einschließlich der Bedingungen für die Skalierbarkeit und für die interne und externe Überprüfbarkeit festzulegen. Dabei berücksichtigt die Kommission spezifische Maßnahmen für Kleinst-, Klein- und mittlere Unternehmen.	Die Ermächtigung der Kommission zur Festlegung von Kriterien und Bedingungen für die genannten Verarbeitungsvorgänge sowie von Anforderungen an die Folgenabschätzung geht zu weit. Diese sollten, soweit sie erforderlich sind, abschließend in der Verordnung geregelt werden. **GDV-Vorschlag:** **Art. 33 Abs. 6 wird gestrichen.**
7. Die Kommission kann Standards und Verfahren für die Durchführung sowie für die interne und externe Überprüfung der in Absatz 3 genannten Folgenabschätzung festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.	Es ist fraglich, ob durch Standardvorlagen ein praktischer Nutzen erreicht werden kann. Diese könnten z.B. den unterschiedlichen Realitäten von Unternehmen widersprechen (z.B. Online- vs. Offline-Tätigkeit). **GDV-Vorschlag:** **Art. 34 Abs. 7 wird gestrichen.**
Artikel 34 ***Vorherige Genehmigung und vorherige Zuratezie-hung***	
1. Der für die Verarbeitung Verantwortliche oder gegebenenfalls der Auftragsverarbeiter holt vor der Verarbeitung personenbezogener Daten eine Genehmigung der Aufsichtsbehörde ein, um sicherzustellen, dass die geplante Verarbeitung in Übereinstimmung mit dieser Verordnung erfolgt, und um insbesondere die Risiken zu mindern, welche für die betroffenen Personen bestehen, wenn dieser Vertragsklauseln nach Artikel 42 Absatz 2 Buchstabe d vereinbart oder keine geeigneten Garantien für die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation in einem rechtsverbindlichen Instrument nach Artikel 42 Absatz 5 vorsieht.	Wenn die Einholung einer vorherigen Genehmigung wirklich nötig ist, so muss der für die Verarbeitung Verantwortliche sie einholen. Da diese Stelle die Verantwortung trägt – und nicht ein etwaiger Auftragsverarbeiter – sollte diese auch den Genehmigungsprozess durchführen. Dies vermindert auch mögliche Missverständnisse und damit Datenpannen bei der Aufsichtsbehörde, falls ein Auftragsverarbeiter für eine größere Anzahl von Auftraggebern tätig ist.
2. Der für die Verarbeitung Verantwortliche oder der in seinem Auftrag handelnde Auftragsverarbeiter zieht vor der Verarbeitung personenbezogener Daten die Aufsichtsbehörde zu Rate, um sicherzustellen, dass die geplante Verarbeitung in Übereinstimmung mit dieser Verordnung erfolgt, und um insbesondere die für die betroffenen Personen bestehenden Risiken zu mindern; dies gilt für alle Fälle, in denen	
a) aus einer Datenschutz-Folgenabschätzung nach Artikel 33 hervorgeht, dass die geplanten Verarbeitungsvorgänge aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke hohe konkrete Risiken bergen können; oder	Mit dieser Regelung würden faktisch in vielen Konstellationen, die unter § 33 der Verordnung fallen, wieder eine Meldepflicht und ein aufsichtsbehördliches Prüfungsverfahren eingeführt. Das gilt unabhängig davon, ob die für die Verarbeitung Verantwortlichen einen Datenschutzbeauftragten eingesetzt haben oder nicht. Gegenüber dem bewährten Verfahren der

	Vorabkontrolle durch den Datenschutzbeauftragten, das in Artikel 20 Abs. 2 der Richtlinie 95/46/EG vorgesehen ist, wäre das ein erheblicher Rückschritt. Mit der Beibehaltung dieses Verfahrens könnten die Bestellung eines Datenschutzbeauftragten belohnt und die Datenschutzbehörden deutlich entlastet werden. **GDV-Vorschlag:** Nachdem Muster des Artikel 20 Abs. 2 der Richtlinie 95/46/EG (in Deutschland umgesetzt in § 4d Abs. 5, 6 BDSG) sollte bei Bestellung eines Datenschutzbeauftragten die Vorabkontrolle durch diesen ausreichen.
b) die Aufsichtsbehörde eine vorherige Zurateziehung bezüglich der in Absatz 4 genannten Verarbeitungsvorgänge, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen können, für erforderlich hält.	Die vorgeschlagene Formulierung lässt der Aufsichtsbehörde zu viel Spielraum, einen Verarbeitungsvorgang als Risiko einzustufen. Es muss bereits in der Verordnung konkret festgeschrieben werden, nach welchen Kriterien ein Verarbeitungsvorgang betrachtet wird, um das Existieren eines hohen Risikos festzustellen. **GDV-Vorschlag:** **Artikel 34 Abs. 2 b wird gestrichen.**
3. Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung nicht im Einklang mit dieser Verordnung steht, insbesondere weil die Risiken unzureichend ermittelt wurden oder eingedämmt werden, untersagt sie die geplante Verarbeitung und unterbreitet geeignete Vorschläge, wie diese Mängel beseitigt werden könnten.	Eine sofortige Untersagung durch die Behörde kann ein unverhältnismäßiger Eingriff sein, der zu erheblichen wirtschaftlichen Schäden führt. Häufig werden mildere Mittel zur Verfügung stehen. Bei den Empfehlungen der Behörden müssen auch die finanziellen und organisatorischen Umstände eines Unternehmens in Betracht gezogen werden, um die Machbarkeit der empfohlenen Maßnahmen zu gewährleisten. **GDV-Vorschlag:** Art. 34 Abs. 3 wird wie folgt formuliert: „Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung nicht im Einklang mit dieser Verordnung steht, insbesondere weil die Risiken unzureichend ermittelt wurden oder eingedämmt werden, ~~untersagt sie die geplante Verarbeitung und~~ unterbreitet **sie** geeignete Vorschläge, wie diese Mängel beseitigt werden könnten. **Bei diesen Vorschlägen wird der technische Fortschritt ebenso in Betracht gezogen wie die, im Hinblick auf die finanzielle und organisatorische Situation der betroffenen Organisation, umsetzbaren Maßnahmen.**“
4. Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, die Gegenstand der vorherigen Zurateziehung nach Absatz 2 Buchstabe b sind, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt derartige Listen an den Europäischen Datenschutzausschuss.	Angesichts der Bedenken gegen Art. 34 Abs. 2 b (dazu oben) ist auch der Wert einer solchen Liste in Zweifel zu ziehen. Wenn sie erstellt werden soll, müssen Datenschutzprinzipien wie auch der Schutz von Geschäftsgeheimnissen beachtet werden, damit keinem Antragssteller Nachteile erwachsen. **GDV-Vorschlag:** **Art. 34 Abs. 4 sollte gestrichen werden.** Zumindest sollte in Art. 34 Abs. 4 am Ende eingefügt werden: „[…] **Bei der beschriebenen Erstellung, Veröffent-**

	lichung und Übermittlung der Liste/n werden zum Schutz der Persönlichkeitsrechte bzw. Geschäftsgeheimnisse der verzeichneten Antragssteller nur anonymisierte und aggregierte Daten verwandt und öffentlich gemacht.“
5. Wenn auf der in Absatz 4 genannten Liste Verarbeitungsvorgänge aufgeführt werden, die sich auf Waren oder Dienstleistungen beziehen, welche betroffenen Personen in mehreren Mitgliedstaaten angeboten werden, oder die dazu dienen sollen, das Verhalten dieser betroffenen Personen zu beobachten, oder die wesentliche Auswirkungen auf den freien Verkehr personenbezogener Daten in der Union haben können, bringt die Aufsichtsbehörde vor der Annahme der Liste das in Artikel 57 beschriebene Kohärenzverfahren zur Anwendung.	Vgl. Anmerkungen zu Art. 34 Abs. 4.
6. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter legt der Aufsichtsbehörde die Datenschutz-Folgenabschätzung nach Artikel 33 vor und übermittelt ihr auf Aufforderung alle sonstigen Informationen, die sie benötigt, um die Ordnungsgemäßheit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Person bestehenden Risiken und die diesbezüglichen Sicherheitsgarantien bewerten zu können.	Vgl. Anmerkungen zu Art. 34 Abs. 2 a.
7. Die Mitgliedstaaten ziehen die Aufsichtsbehörde bei der Ausarbeitung einer von ihren nationalen Parlamenten zu erlassenden Legislativmaßnahme oder einer sich auf eine solche Legislativmaßnahme gründenden Maßnahme, durch die die Art der Verarbeitung definiert wird, zu Rate, damit die Vereinbarkeit der geplanten Verarbeitung mit dieser Verordnung sichergestellt ist und insbesondere die für die betreffenden Personen bestehenden Risiken gemindert werden.	
8. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die Bestimmung der in Absatz 2 Buchstabe a genannten hohen konkreten Risiken festzulegen.	Siehe Bedenken zu Art. 34 Abs. 2 a. **GDV-Vorschlag:** **Art. 34 Abs. 8 wird gestrichen.**
9. Die Kommission kann Standardvorlagen und Verfahrensvorschriften für die in den Absätzen 1 und 2 genannte vorherige Genehmigung beziehungsweise Zurateziehung sowie für die in Absatz 6 vorgesehene Unterrichtung der Aufsichtsbehörde festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen.	

ABSCHNITT 4
DATENSCHUTZBEAUFTRAGTER

Artikel 35 ***Benennung eines Datenschutzbeauftragten***	EG 75.
1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen einen Datenschutzbeauftragten, falls	Wichtig erscheint es, Anreize für die Bestellung eines Datenschutzbeauftragten zu schaffen, wie z.B. die Vorabkontrolle risikoreicher Datenverarbeitungen ohne Einschaltung der Aufsichtsbehörde. Die umständliche Folgenabschätzung nach Art. 33 und die unsichere und bürokratische Konsultation der Aufsicht nach Art. 34 könnten so durch ein bewährtes Verfahren ersetzt werden, dass die Aufsichtsbehörden im Ergebnis entlastet (siehe Anmerkungen zu Art. 34).
a) die Verarbeitung durch eine Behörde oder eine öffentliche Einrichtung erfolgt; oder	
b) die Bearbeitung durch ein Unternehmen erfolgt, das 250 oder mehr Mitarbeiter beschäftigt, oder	Über die Grenze kann sicher gestritten werden. Jedenfalls erscheint es nicht sinnvoll, für kleine Unternehmen (unter 9 Mitarbeiter, die mit Datenverarbeitung beschäftigt sind) einen Datenschutzbeauftragten vorzusehen, da in der Regel die Geschäftsführung den Gesamtüberblick hat und auch das Thema Datenschutz mit abdecken wird.
c) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen.	
2. Im Fall des Absatzes 1 Buchstabe b darf eine Gruppe von Unternehmen einen gemeinsamen Datenschutzbeauftragten ernennen.	
3. Falls es sich bei dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder um eine öffentliche Einrichtung handelt, kann der Datenschutzbeauftragte unter Berücksichtigung der Struktur der Behörde beziehungsweise der öffentlichen Einrichtung für mehrere Bereiche benannt werden.	
4. In anderen als den in Absatz 1 genannten Fällen können der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Gremien, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen.	
5. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter benennt den Datenschutzbeauftragten nach Maßgabe der beruflichen Qualifikation und insbesondere des Fachwissens, das dieser auf dem Gebiet des Datenschutzrechts und der einschlägigen Praktiken besitzt, sowie nach Maßgabe von dessen Fähigkeit zur Erfüllung der in Artikel 37 genannten Aufgaben. Der Grad des erforderlichen Fachwissens richtet sich insbesondere nach der Art	

der durchgeführten Datenverarbeitung und des erforderlichen Schutzes für die von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten.	
6. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass etwaige sonstige berufliche Pflichten des Datenschutzbeauftragten mit den Aufgaben und Pflichten, die diesem in seiner Funktion als Datenschutzbeauftragter obliegen, vereinbar sind und zu keinen Interessenkonflikten führen.	
7. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter benennt einen Datenschutzbeauftragten für einen Zeitraum von mindestens zwei Jahren. Der Datenschutzbeauftragte kann für weitere Amtszeiten wiederernannt werden. Während seiner Amtszeit kann der Datenschutzbeauftragte seines Postens nur enthoben werden, wenn er die Voraussetzungen für die Erfüllung seiner Pflichten nicht mehr erfüllt.	
8. Der Datenschutzbeauftragte kann durch den für die Verarbeitung Verantwortlichen oder durch den Auftragsverarbeiter beschäftigt werden oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.	
9. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter teilt der Aufsichtsbehörde und der Öffentlichkeit den Namen und die Kontaktdaten des Datenschutzbeauftragten mit.	
10. Betroffene Personen haben das Recht, den Datenschutzbeauftragten zu allen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten stehenden Fragen zu Rate zu ziehen und die Wahrnehmung ihrer Rechte gemäß dieser Verordnung zu beantragen.	
11. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in Absatz 1 Buchstabe c genannte Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters sowie die Kriterien für die berufliche Qualifikation des in Absatz 5 genannten Datenschutzbeauftragten festzulegen.	
Artikel 36 ***Stellung des Datenschutzbeauftragten***	
1. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.	
2. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass der Datenschutzbeauftragte seinen Pflichten und Aufgaben unabhängig nachkommen kann und keine Anweisungen bezüglich der Ausübung seiner Tätigkeit erhält. Der Datenschutzbeauftragte berichtet unmittelbar der Leitung des für die Verarbeitung Verantwort-	

lichen oder des Auftragsverarbeiters.	
3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben und stellt das erforderliche Personal, die erforderlichen Räumlichkeiten, die erforderliche Ausrüstung und alle sonstigen Ressourcen, die für die Erfüllung der in Artikel 37 genannten Pflichten und Aufgaben erforderlich sind, zur Verfügung.	
Artikel 37 ***Aufgaben des Datenschutzbeauftragten***	
1. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter betraut den Datenschutzbeauftragten mit mindestens folgenden Aufgaben:	
a) Unterrichtung und Beratung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters über dessen aus dieser Verordnung erwachsenden Pflichten sowie Dokumentation dieser Tätigkeit und der erhaltenen Antworten;	
b) Überwachung der Umsetzung und Anwendung der Strategien des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;	
c) Überwachung der Umsetzung und Anwendung dieser Verordnung, insbesondere ihrer Anforderungen an einen Datenschutz durch Technik und an datenschutzfreundliche Voreinstellungen, an die Datensicherheit, an die Benachrichtigung der betroffenen Personen und an die Anträge der betroffenen Personen zur Wahrnehmung der ihren nach dieser Verordnung zustehenden Rechte;	
d) Sicherstellung, dass die in Artikel 28 genannte Dokumentation vorgenommen wird;	
e) Überwachung der Dokumentation und Meldung von Verletzungen des Schutzes personenbezogener Daten sowie die Benachrichtigung davon gemäß den Artikeln 31 und 32;	
f) Überwachung der von dem für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter durchgeführten Datenschutz-Folgenabschätzung sowie der Beantragung einer vorherigen Genehmigung beziehungsweise Zurateziehung gemäß den Artikeln 33 und 34;	
g) Überwachung der auf Anfrage der Aufsichtsbehörde ergriffenen Maßnahmen sowie Zusammenarbeit im Rahmen der Zuständigkeiten des Datenschutzbeauftragten mit der Aufsichtsbehörde auf deren Ersuchen oder auf eigene Initiative des Datenschutzbeauftragten;	
h) Tätigkeit als Ansprechpartner für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen sowie gegebenenfalls Zurateziehung der	

Aufsichtsbehörde auf eigene Initiative.	
2. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die Aufgaben, die Zertifizierung, die Stellung, die Befugnisse und die Ressourcen des in Absatz 1 genannten Datenschutzbeauftragten festzulegen.	Die Kommission ist in keiner Weise kompetent und berechtigt, die in Art. 37 Abs. 2 erwähnten Kriterien und Anforderungen festzulegen, da diese die Organisationsstruktur von Unternehmen betreffen. Insbesondere kann sie nicht Bestimmungen zur Ressourcenausstattung, d.h. zur Finanzierung des Datenschutzbeauftragten festlegen, da die dahingehenden Details in der Entscheidungsgewalt des anstellenden Unternehmens liegen. **GDV-Vorschlag:** **Art. 37 Abs. 2 wird gestrichen.**