Zusammenfassung der Stellungnahme zum Vorschlag der EU-Datenschutzverordnung

KOM(2012) 11/4

vom 25. Januar 2012

Die **deutsche Versicherungswirtschaft unterstützt** die Ziele, das **Datenschutzrecht in Europa zu vereinheitlichen**, die grenzüberschreitende Tätigkeit zu erleichtern und Hemmnisse für den internationalen Datentransfer zu beseitigen.

Angesichts des ohnehin schon hohen Datenschutzstandards sollte eine Regelung der Rechte der Betroffenen und der Anforderungen an Datenschutz und Datensicherheit jedoch **mit Augenmaß** erfolgen und **unnötige bürokratische Belastungen vermeiden**. Regelungen, die erkennbar von Vorfällen in der Internetwirtschaft angestoßen sind und nur für den Bereich des Internets Sinn ergeben, sollten dabei nicht generell und allgemeingültig gemacht werden.

Im Hinblick auf **versicherungsspezifische Geschäftsabläufe** enthält der Vorschlag der Datenschutz-Grundverordnung noch **erhebliche rechtliche Unsicherheiten** sowie Bestimmungen, die die Bereitstellung von Versicherungsschutz erheblich erschweren, verteuern und in Teilen sogar gefährden würden.

Die zukünftige Verordnung sollte insbesondere folgende Punkte berücksichtigen:

1) Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten

Der Vorschlag enthält bisher keine ausreichende gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft. In der Lebens-, Kranken-, Unfall-, Haftpflicht- und Rückversicherung werden Gesundheitsdaten zwingend benötigt, um im Einklang mit versicherungsaufsichtsrechtlichen Bestimmungen die zu versichernden Risiken zu prüfen und Versicherungsfälle abwickeln zu können.

Beispiel:

- Ein Krankenrücktransport aus dem Ausland kann nur organisiert werden, wenn dem Versicherer oder Assisteur, der den Transport organisiert, bekannt ist, welche Erkrankung der Versicherte hat.

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5290
Fax: +49 30 2020-6290

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +32 2 28247-39

Ansprechpartner:
Dr. Martina Vomhof
Leiterin
Datenschutz/Grundsatzfragen

E-Mail: m.vomhof@gdv.de

www.gdv.de

Eine Einwilligung als Rechtsgrundlage birgt Unsicherheiten u. a. aus folgenden Gründen:

Der Verordnungsvorschlag geht davon aus, dass die **betroffene Person ihre Einwilligung jederzeit widerrufen kann** (Art. 7 Abs. 3 und Erwägungsgrund 32). Eine Vertragsdurchführung ohne Verarbeitung der Daten ist aber nicht möglich.

Nach Art. 7 Abs. 4 ist die Einwilligung als Rechtsgrundlage der Datenverarbeitung ausgeschlossen, wenn **zwischen dem Betroffenen und der verantwortlichen Stelle ein erhebliches Ungleichgewicht** besteht. Es ist zu erwarten, dass Datenschutzbehörden ein solches Ungleichgewicht nicht nur in Beschäftigungsverhältnissen (Erwägungsgrund 34) sondern auch zwischen Versicherungsunternehmen und ihren Kunden oder Geschädigten annehmen. Damit wäre eine Einwilligung ausgeschlossen.

Position der deutschen Versicherungswirtschaft:

Notwendig ist eine eindeutige, europaweit geltende gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten in allen betroffenen Versicherungssparten.

2) Abgrenzung von der Profilbildung

Der Vorschlag verbietet in Art. 20 grundsätzlich Profilbildungen aufgrund automatisierter Prozesse. Damit soll in erster Linie die Bildung von Verhaltensprofilen aufgrund von Aktivitäten im Internet verhindert werden. Die Bestimmung würde nach ihrem Wortlaut jedoch auch **automatisierte Tarifeinstufungen und Risikoeinschätzungen in der Versicherungswirtschaft erfassen** und damit die **Arbeit der Versicherungswirtschaft im Kern gefährden**.

Es entspricht der **Natur von Versicherungsverträgen**, dass **nach bestimmten Kriterien Risikogemeinschaften gebildet** werden müssen.

Beispiel:

- In der Elementarschadenversicherung können Häuser, die in einem in regelmäßigen Abständen von Überschwemmungen betroffenen Ort liegen, nicht zu gleichen Konditionen versichert werden wie Häuser, die in einem Ort fernab von Gewässern liegen.

Eine ordnungsgemäße Geschäftsorganisation eines Versicherers setzt nach Art. 44 der Solvency II-Rahmenrichtlinie (RL 2009/138/EG) ein angemessenes Risikomanagement voraus. Im Rahmen der erforderlichen Risikosteuerung ist die Tarifierung und Risikoeinschätzung zwingend erforderlich.

Position der deutschen Versicherungswirtschaft:

Tarifierung und Risikoeinschätzung in der Versicherungswirtschaft müssen ausdrücklich vom Begriff der Profilbildung in Art. 20 ausgenommen werden.

3) Verhinderung von Versicherungsbetrug und Gewährleistung der Zuverlässigkeit von Versicherungsvermittlern

Für den **Betrieb von Auskunfteien** gibt es im Vorschlag für die EU-Datenschutzgrundverordnung **keine klare gesetzliche Grundlage**. Denn Art. 6 Abs. 1f. erlaubt – anders als Art. 7f) der RL 95/46/EG – keine Datenverarbeitung im Interesse Dritter. Außerdem fehlt eine Erlaubnis für die Verarbeitung von Daten über Straftaten direkt in der Verordnung (vgl. Art. 9 Abs. 1, 2).

Die Versicherungswirtschaft benötigt Auskunfteien zum Schutz vor Versicherungsbetrug und unseriösen Versicherungsvermittlern.

Beispiele:

- In Deutschland werden im **Hinweis- und Informationssystem (HIS)** bestimmte, auf ein erhöhtes Risiko hindeutende Daten aus den Versicherungsunternehmen gespeichert. Dazu gehören auch Verurteilungen wegen Versicherungsbetrugs.
- Die **Auskunftsstelle über den Versicherungs- und Bausparaußendienst (AVAD)** verarbeitet Informationen über Vermittler, um im Interesse der Verbraucher deren Zuverlässigkeit sicherzustellen.

Position der deutschen Versicherungswirtschaft:

Der Betrieb der genannten Systeme muss sichergestellt werden, indem eine **Datenverarbeitung im Interesse Dritter zugelassen** wird sowie eine **Verarbeitung von Daten über Strafurteile bei erheblichem berechtigtem Interesse** unmittelbar aufgrund der Verordnung ermöglicht wird.

4) Datenschutzfolgenabschätzung als eine unnötige bürokratische Belastung

Neben anderen **erheblichen neuen bürokratischen Belastungen** (z. B. Art. 22, 23, 28, 29 und 30) enthält **Art. 33 zusätzlich das Erfordernis einer Datenschutzfolgenabschätzung**. Inhalt und Umfang der Folgenabschätzung werden nicht deutlich. Zusätzlich wird **nicht klar, warum und in welchen Fällen die Aufsichtsbehörde konsultiert werden muss** (Art. 34 (2)). Jedoch sollen Sanktionen verhängt werden, wenn die Datenschutzfolgenabschätzung nicht durchgeführt oder die Aufsichtsbehörde nicht konsultiert wird (Art. 79 (6) (i)). Hinzu kommt, dass die Betroffenen

zu konsultieren sind. Das verlangt das Offenlegen von Geschäftsgeheimnissen.

Für Versicherungsunternehmen würde die Folgenabschätzung zur Regel. Dies bedeutet nicht nur Verwaltungsaufwand, sondern Rechtsunsicherheit.

Position der deutschen Versicherungswirtschaft:

Da die Auswirkungen einer Datenverarbeitung für die Betroffenen ohnehin im Rahmen anderer Anforderungen beachtet werden müssen, sind Art. 33 und 34 Abs. 2 entbehrlich.

5) Weitere Anliegen der deutschen Versicherungswirtschaft

- Umfangreiche Betroffenenrechte, wie das **Recht auf Vergessen** (Art. 17) und **Datenübertragbarkeit** (Art. 18), die primär auf soziale Netzwerke im Internet zugeschnitten sind, können nicht 1:1 in die Offline-Welt übertragen werden. Sie dürfen insbesondere die Vertragsdurchführung nicht gefährden.

- Möglichkeiten zur **kollektiven Rechtsdurchsetzung** sind nicht erforderlich, zumal den Datenschutzaufsichtsbehörden weitgehende Kompetenzen eingeräumt sind.

- **Sanktionen** sollten auf ein verträgliches Maß begrenzt werden und nicht losgelöst von der Auswirkung des Verstoßes anfallen.

- Die weiten Befugnisse der Europäischen Kommission zum **Erlass von delegierten Rechtsakten** bedeuten Rechtsunsicherheit. Vorzugswürdig ist eine Konkretisierung der Verordnung durch branchenspezifische Selbstregulierungsmaßnahmen.

- Die **Verpflichtung zur Meldung** jeder Zerstörung, jedes Verlusts, jeder Veränderung und jedes unberechtigten Zugriffs auf personenbezogene Daten ist zu strikt ausgestaltet. Ein so weit gefasster Anwendungsbereich lässt eine Meldeflut bei den Aufsichtsbehörden und eine Abstumpfung der immer wieder auch in nichtigen Fällen benachrichtigten Betroffenen befürchten. Art. 31 und 32 sollten so eingeschränkt werden, dass nur besonders schutzwürdige Daten und 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.

Berlin, 12. Juni 2012

Executive Summary of comments

on the proposal for an EU Data Protection Regulation

COM(2012) 11/4

of 25 January 2012

The **German insurance industry supports the harmonization of data protection law in Europe** to facilitate cross-border activities and to remove obstacles to international data transfer.

However, given already high data protection standards, rules on the rights of data subjects and on the requirements for data protection und data security should be **proportionate**, thus **avoiding unnecessary bureaucratic burdens**. Rules which have clearly been influenced by incidents in the internet business and only make sense for this domain should not be universally implemented.

With respect to **insurance-specific business processes**, the proposal for a General Data Protection Regulation contains **substantial legal uncertainties** and could make the provision of insurance cover considerably more difficult and expensive and partly even jeopardize it.

The future regulation should particularly take the following points into consideration:

1) Legal basis for the processing of health data

The regulation proposal does not provide a sufficient legal basis for the processing of health data in the insurance industry. In health, life, accident and third party liability insurance as well as reinsurance, this type of data is imperatively needed to assess risks to be insured and settle claims in line with the provisions of insurance supervisory law.

Example:

- A medical evacuation from abroad can only be organized if the disease of the insured is known to the insurer or assistor organizing the evacuation.

The possible use of declarations of consent as a legal basis holds uncertainties due to the following reasons:

The proposal assumes that the **data subject may withdraw his or her consent at any time** (Art. 7 (3) and recital 32). However, performance of the contract without processing of the data is impossible.

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

German Insurance Association

Wilhelmstraße 43 / 43 G, D - 10117 Berlin
PO Box 08 02 64, D - 10002 Berlin
Phone: +49 30 2020-5290
Fax: +49 30 2020-6290

51, rue Montoyer
B - 1000 Bruxelles
Phone: +32 2 28247-30
Fax: +32 2 28247-39

Contact:
Dr. Martina Vomhof
Head of Data Protection/Basic Issues

E-mail: m.vomhof@gdv.de

www.gdv.de

Moreover, the admissibility of declarations of consent in the insurance industry is called into question by Art. 7 (4). According to this paragraph, consent is excluded as a legal basis for data processing where there is a significant **imbalance between the data subject and the controller**. It can be expected that data protection authorities will assume that such an imbalance exists not only between employers and employees (recital 34), but also between insurance companies and their customers. Thus, any consent would be excluded.

Position of the German insurance industry:

There is need for a clear Europe-wide legal basis for the processing of health data in all insurance lines concerned.

2) **Delimitation from profiling**

Art. 20 of the regulation proposal generally prohibits profiling based on automated processes. This is primarily intended to prevent the creation of behaviour profiles based on activities on the internet. However, the provision would also **cover automated rate classification and risk assessment in the insurance industry, thus jeopardizing the essence of its activities**.

It is in the **nature of insurance contracts that risk communities have to be formed according to certain criteria**.

Example:

- In natural disaster insurance, houses situated in a location which is affected by floods at regular intervals cannot be insured on the same terms as houses situated in a location far away from waters.

According to Art. 44 of the Solvency II Framework Directive (Directive 2009/138/EC), proper business organization of an insurer presupposes adequate risk management. Within the scope of necessary risk management, rating and risk assessment are imperative.

Position of the German insurance industry:

Rating and risk assessment in the insurance industry should be explicitly excluded from the concept of profiling as referred to in Art. 20.

3) **Prevention of insurance fraud and ensuring the reliability of intermediaries**

The proposal for an EU Data Protection Regulation **does not provide for a clear legal basis for the operation of information offices**. It is uncertain whether Art. 6 (1) (f) is to cover these cases because this rule falls

short of Art. 7 (f) of Directive 95/46/EC, which also covers data processing in the interest of third parties. In addition, the proposal lacks a direct admission of processing of data on criminal offences (cf. Art. 9 (1) and (2)).

The insurance industry requires the assistance of information offices for protection against insurance fraud and unreliable intermediaries.

Examples:

- In Germany, the **Detection and Information System** (Hinweis- und Informationssystem - HIS) stores specific data from insurance companies which suggest increased risk. In clearly defined cases, there may be a data exchange between insurance companies concerned. HIS also stores convictions due to insurance fraud, which may be queried by other insurers.
- The **Information Office on the Insurance and Buildings Societies' Field Service** (Auskunftsstelle über den Versicherungs- und Bausparaußendienst - AVAD) processes information on intermediaries to ensure their reliability in the interest of consumers.

Position of the German insurance industry:

The operation of the systems mentioned should be ensured by allowing **data processing in the interest of third parties**. Furthermore, **processing of data on criminal convictions should be possible in case of significant legitimate interest**.

4) Impact assessment as an unnecessary bureaucratic burden

Although the regulation entails **considerable new bureaucratic burdens** (e.g. in Art. 22, 23, 28, 29 and 30), **Art. 33 additionally holds the obligation for an impact assessment**. It is not calculable, in which cases the rule applies. Furthermore, the intended content and scope of the impact assessment are unclear. Additionally it is **not obvious, why and in which cases the supervisory authority has to be consulted** (Art. 34 (2)). Nevertheless sanctions are to be imposed in case of non-compliance with the requirement to carry out the impact assessment and to consult the supervisory authority (Art. 79 (6) (i)). The assessment of data subjects is also required. This jeopardizes business secrets.

For insurance companies, the impact assessment would become a rule rather than an exception. This would represent not only an administrative burden, but also legal insecurity.

Position of the German insurance industry:

Since the effects of data processing for data subjects have to be observed anyway within the scope of other requirements, Art. 23 and 33 are dispensable.

5) Further concerns of the German insurance industry

• Extensive rights of data subjects, such as the **right to be forgotten** (Art. 17) or the **right to data portability** (Art. 18), which are primarily tailored to social networks on the internet, cannot be absolutely applied to the offline world. They should not jeopardize the performance of contracts.

• Possibilities for **collective redress** are not required, especially since data protection authorities have been granted extensive powers. Sanctions should be limited to a reasonable extent.

• **Sanctions** must be limited to an agreeable degree and directly linked to the magnitude of the offence's consequences.

• The extensive powers granted to the Commission regarding the issue of **delegated legal acts** cause legal uncertainty. It would be preferable to concretize the regulation by means of sector-specific measures of self-regulation.

• The **obligation to report data breaches** in case of any destruction, loss, alteration of or unauthorized access to personal data is too strict. A scope defined this broadly may cause a flood of reports with supervisory authorities. Data subjects, who are notified time and again also in trivial cases, may become indifferent to them. Articles 31 and 32 should be restricted to the extent that they cover only data which deserve specific protection and only unlawful transfer when there is a risk of severe infringements of the rights or interests deserving protection of data subjects. Section 42a, which has been inserted into the German Federal Data Protection Act in 2009, may serve as a model.

Berlin, 12 June 2012

Comments

on the proposal for an EU Data Protection Regulation

COM(2012) 11/4

of 25 January 2012

Summary

The German insurance industry supports the harmonization of data protection law in Europe, to facilitate cross-border activities and to remove obstacles to international data transfer.

However, given already high data protection standards, e.g. in Germany, rules on the rights of data subjects and on the requirements for data protection und data security should be proportionate, thus avoiding unnecessary bureaucratic burdens. Rules which have clearly been influenced by incidents in the Internet business and only make sense for this area should not be implemented at a general or universal level.

With respect to insurance-specific business processes, the proposal for a General Data Protection Regulation retains substantial legal uncertainties as well as provisions which would make the provision of insurance cover considerably more difficult and expensive and partly even jeopardize it.

The future regulation should in particular allow for the following points:

- There is need for a clear **legal basis for the processing of health data** in life, health, accident and third party liability insurance as well as reinsurance. It should also cover **data processing operations within a group and with the involvement of specialized service providers**, which are meanwhile common practice and appropriate (see Section 1).

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

German Insurance Association

Wilhelmstraße 43 / 43 G, D - 10117 Berlin
PO Box 08 02 64, D - 10002 Berlin
Phone: +49 30 2020-5290
Fax: +49 30 2020-6290

51, rue Montoyer
B - 1000 Bruxelles
Phone: +32 2 28247-30
Fax: +32 2 28247-39

Contact:
Dr. Martina Vomhof
Head of
Data Protection/Basic Issues

E-mail: m.vomhof@gdv.de

www.gdv.de

- Risk-based pricing and risk differentiation as core elements of the insurance business should remain possible. The provisions on **profiling** (Art. 20), which are tailored to the Internet, should not cover rate classification and risk assessment in the insurance industry. The **definitions** should be revised to the effect that the use of less sensitive data on objects and of pseudonymized data remains possible (see Section 2).
- Procedures for **protection against insurance fraud and unreliable insurance intermediaries** should remain operable (see Section 3).
- Extensive **rights of data subjects**, such as the right to be forgotten (Art. 17) or the right to data portability (Art. 18), which are primarily tailored to social networks on the internet, should not jeopardize the performance of contracts (see Section 4).
- The **requirements for measures on data protection and security** should remain practical (see Section 5). The data protection impact assessment (Art. 33), which represents a considerable burden, should be deleted and the obligation to report data breaches should be restricted to serious cases (Articles 31, 32).
- Possibilities for **collective redress** are not required, especially since data protection authorities have been granted extensive powers (see Section 7). **Sanctions** should be limited to a reasonable extent (Section 8).
- The extensive powers granted to the European Commission regarding the **issue of delegated legal acts** cause legal uncertainty. It would be preferable to concretize the regulation by means of sector-specific **measures of self-regulation** (see Section 9).

Contents

Preliminary remarks

As a risk taker for companies and private households, the insurance industry fulfils an essential function within the scope of the entire economy. Like individual provisions or state-organized protection, the possibility to protect oneself through private insurance cover against the basic risks of life is one of the cornerstones of provision for elementary requirements in a social market economy. By assuming private or public risks, the insurance industry creates the security which is necessary for companies and the economy so that initiative and innovative free enterprise may develop in the first place. Protection against private risks of life enables citizens to live in freedom and security.

In Germany alone, insurance companies offer comprehensive coverage and social security through approx. 450 million insurance contracts.

German insurers are aware of their responsibility, which is accompanied by the fact that they have to process personal data of their customers and proposers to fulfil their tasks. For this reason, the German Insurance Association (*Gesamtverband der Deutschen Versicherungswirtschaft - GDV*), in cooperation with the German data protection authorities, is currently preparing a code of conduct for the handling of personal data. This envisaged self-regulation measure is closely linked to a declaration of consent under data protection law for life and health insurance, which has been jointly prepared and has been recommended by the German data protection authorities since January 2012 and also comprises the release from confidentiality required under German criminal law. *Verbraucherzentrale Bundesverband* (*vzbv* – “Federal Association of Consumer Advice Centres”), being the most important lobbying institution of consumers in Germany, is also involved in the preparation of the code of conduct and the declaration of consent. Thus, the insurance industry will be the first sector in Germany to have a data protection concept which is supported jointly by data protection authorities, consumer protectors and the business community.

Against this background, the German insurance industry welcomes the efforts made by the European Commission to harmonize data protection law in Europe. For companies operating on a European scale, it represents a considerable relief if they do not have to deal with different material data protection regulations.

Incentives for implementation of codes of conduct (Art. 38) and binding corporate rules (Art. 43) are appropriate. However, the requirements with respect to content should not be defined too rigidly so as to ensure widespread acceptance and practicability.

From the point of view of the insurance industry, the future regulation should allow, in particular, for the following points:

1. Processing of health data in the insurance industry

a) Legal basis for the processing of health data

A clear legal basis is required for the processing of health data in life, health, accident, third party liability insurance and reinsurance.

Background:

In health insurance, life insurance and accident insurance health data are imperatively needed to assess risks to be insured and settle claims in line with the provisions of insurance supervisory law.

Examples:

- Whether an insured is entitled to an occupational disability annuity can only be ascertained when it has been checked whether he has a disease due to which he is no longer able to exercise his occupation.
- A medical evacuation from abroad can only be organized if the disease of the insured is known to the insurer or assistor organizing the evacuation.
- Reinsurers assuming risks in whole or in part from direct insurers, thus ensuring the fulfilment of contracts, need health data to check whether they may accept the risk or may be made liable for it in the event of a claim.
- Third party liability insurers may settle bodily injury claims only if they are allowed to process health data of victims.

The objective must be to put the processing of health data in the insurance industry, which is necessary for the social protection of the public, on a legally certain basis. It should allow for the interests of insureds and customers applying for insurance cover, which include efficient processes within the scope of risk assessment and claim settlement.

Commission proposal for a Regulation:

So far the proposal does **not** provide a **sufficient legal basis for the processing of health data in the insurance industry**. Such a legal basis is urgently required for the insurance sector, also in the opinion of the German data protection authorities.

Although the proposal includes many starting points which might provide a **legal basis** for the necessary processing of health data, these are insufficient:

- Art. 9 (2) (f) deals with processing for the establishment, exercise or defence of legal claims, but not (like Art. 6 (1) (b)) for the establishment and performance of contracts.
- Art. 9 (2) (g) is not likely to be applied if Art. 9 (2) (h) in conj. with Art. 81 of the regulation are understood to be special permissive rules for the processing of health data.
- According to Art. 9 (2) (h), the processing of health data is admissible if it is necessary for "*health purposes*" subject to the conditions and safeguards referred to in Art. 81. This covers, if anything, health insurance. Furthermore, given the wording of Art. 81 (1) (c), it is uncertain whether or not this is the case.

The use of **declarations of consent** as a legal basis is only the second best solution. It does not allow for actual business processes and will ultimately lead to a deterioration of the situation of policyholders.

The proposal assumes that the data subject enjoys complete freedom of decision and may **withdraw his or her consent at any time** (Art. 7 (3) and recital 32). If data have to be processed for the performance of a contract, the customer may theoretically refrain from conclusion of the contract. However, performance of the contract without processing of the data is impossible. Furthermore, data processing according to predetermined automated processes has meanwhile become common practice and serves to handle millions of contracts. It is thus not realistic that individual data subjects would influence the manner of processing.

Moreover, the admissibility of declarations of consent in the insurance industry is challenged by **Art. 7 (4)** of the regulation proposal. According to this paragraph, **consent is excluded** as a legal basis for data processing where there is a **significant imbalance** between the data subject and the controller. According to recital 34, this is the case where the data subject is in a situation of dependence, e.g. in employment relationships. In the opinion of data protection authorities, it cannot be ruled out that such an imbalance is assumed not only between employers and employees, but also between insurance companies and their customers. Thus, any consent would be excluded. A general exclusion of consent in Art. 7 (4) restricts consumers in their freedom of decision and conflicts with the actual purpose of data protection, namely to strengthen the position of individuals as those in control of their data. It confronts the insurance industry with great difficulties in justifying its data processing.

<u>Position of the German insurance industry:</u>

There is need for a clear Europe-wide legal basis for the processing of health data in all insurance lines concerned, i.e. in life, health, accident and third party liability insurance as well as reinsurance. Such a legal basis should also cover the processing of data on an intercompany basis in a

group and the involvement of third parties, such as medical experts and assistance companies (see below, Section 2).

b) Processing of health data in a group and involvement of service providers

There is need for a legal basis for the processing of health data in a group and the involvement of service providers.

Background:

To achieve synergies and to meet the requirement of efficiency, it is necessary in insurance groups as well as in other sectors to delegate and centralize service tasks or to outsource them to competent service providers.

Examples:

- The acceptance of notifications of loss, the monitoring of claim settlement and the control of orders for expert opinions are assumed by a certain company of the group or a specialized service provider.
- A company delegates the entire risk assessment and claims handling for all companies of the group to staff members of the parent company.
- For instance, in smaller companies diseases are always appraised by external physicians and in large companies this is done in certain cases.
- Patient care abroad and medical evacuations are carried out by assistance companies specialized on this.
- The supply with medical aids and appliances takes place through specialized companies.

These measures as well as risk shifting towards reinsurers are permitted according to Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 (on the taking-up and pursuit of the business of Insurance and Reinsurance – Solvency II) under insurance supervisory law.

Proposal of the Commission:

Art. 4 (5) and Art. 24 are not helpful for the regulation of joint data processing because they do not create a clear authorization basis for disclosures from one controller to another. Many data protection authorities believe that as soon as an entire task is delegated, contract data is no longer processed on behalf of the entity originally possessing said data but rather that responsibility is completely transferred, so that Art. 26 is not applicable.

Thus, as a matter of principle, where health data are processed, a **declaration of consent** by the data subject is needed for every data transfer operation. Leaving aside the significant legal uncertainties involved in

such consent (see above 1a) and the associated expenditure in terms of time and costs, this approach proves to be extremely impractical for all alterations during the term of an insurance contract. According to experience, after conclusion of the contract, the majority of data subjects simply do not react to the request to give their consent. Given the need for alterations of business processes, it is impossible to ask every single policyholder time and again to give his or her consent.

In the insurance industry, these problems cannot simply be solved by combining companies, thus transforming them into a single controller. In fact, according to Art. 73 of Directive 2009/138/EC, insurance companies are, as a matter of principle, bound to observe the principle of **separation of business lines** between life and non-life insurance. These insurance lines may only be carried on by different legal entities. In Germany, the requirement of separation of lines also applies to substitutive health insurance and to claims handling in legal expenses insurance. These rules only serve to separate recoverable assets and have no reason in terms of data protection.

Position of the German insurance industry:

Instead of a declaration of consent, which is given by many data subjects without reflection and therefore often does not provide any special protection, it would be reasonable to create legal requirements for admissibility of data transfer operations between companies of an insurance group, to reinsurance companies and service providers. If it is ensured that the data are processed only in line with the original purpose, that the other companies have been carefully selected, taking account of the suitability of the technical and organizational measures taken by them for the purposes of data protection and data security, and that, furthermore, it has been contractually agreed that the protection of confidential information and data protection are ensured with the other company, even the transfer of health data should be allowed.

This legal solution would protect all data subjects, regardless of whether or not they give their consent.

c) Processing of genetic and biometric data in the insurance industry

aa) Genetic data

The processing of genetic data, which is necessary in the insurance business, should be possible on a secure legal basis.

Background:

The conduct of genetic tests is not required by German insurers either before or after the conclusion of an insurance contract. The results of existing genetic tests are used within the bounds of what is legally allowed only in the case of conclusion of contracts with very high premiums. However, disclosure of known pre-existing diseases subject to the provisions of the relevant insurance contract law should remain possible.

Today, besides conventional examination methods, the evaluation of genetic data frequently plays a role within the scope of medical diagnoses. For instance, the type of a cancer disease and the way how it may be treated may be determined both conventionally and by means of genetic tests. The insurance industry requires examination results for risk assessment and claims handling in personal insurance. The use of these data for examining an existing diagnosed disease should not depend on the examination method used by a physician.

Commission proposal for a Regulation:

According to Art. 4 (10), 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development. This concept of genetic data is too wide. It covers, for instance, also sex, which is visible to everyone. Furthermore, it also covers disabilities which are not genetically determined, but have been acquired during pregnancy, for instance, due to lack of oxygen.

Art. 9 (1) includes 'genetic data' in the special categories of personal data without defining sufficient exceptions.

Position of the German insurance industry:

The concept of 'genetic data' in Art. 4 (10) should be limited to data on genetic characteristics of any person which have been obtained through examination of the DNA, the RNA or the chromosomes.

However, the use of genetic data for examining an existing, diagnosed disease should be possible just as the use of the results of conventional examination methods because the methods used by a physician cannot be influenced. Therefore, genetic data should be treated like health data.

bb) Biometric calculation bases

The concept of biometric data should be clearly limited to 'biometric identification data'.

In medico-actuarial science, so-called “biometric calculation bases” play a role, which means that physical or physiological characteristics are included in actuarial calculations. This is not likely to be meant in Art. 4 (11). However, there might be confusion with the biometric identification data, which are meant here.

2. Risk-based pricing and risk assessment in the insurance industry

a) Delimitation from profiling

Risk-based pricing and risk assessment in the insurance industry should be explicitly excluded from the concept of profiling as referred to in Art. 20.

Background:

It is in the nature of insurance contracts that risk communities have to be formed according to certain criteria. Usually this happens based on the statistical evaluation of known claims. These are grouped according to common characteristics and thus reveal the statistically probable claims development of the category of characteristics. This method is employed in case of the mortality tables used in the insurance industry. The probability of occurrence of a claim and its extent are assessed on a case-by-case basis by means of a risk assessment based on the information provided by the policyholder and using company statistics and other known probabilities, such as medical experience. The price of insurance cover is fixed according to this classification.

Examples:

- In natural disaster insurance, houses situated in a location which is affected by floods at regular intervals cannot be insured on the same terms as houses situated in a location far away from waters.
- Likewise, the assessment of the premium differs according to whether a house to be insured has a highly combustible thatched roof or a fire-proof shingle roof.
- A hobby pilot cannot be insured on the same terms as somebody who has no dangerous hobby.
- In occupational disability insurance, a person with a serious spinal disease can only be insured on more unfavourable terms because it is more likely that the community of insured persons will have to face costs.

Data processing in the insurance industry is regulated in detail in Recommendation Rec(2002)9 of the Committee of Ministers of the Council of Europe to Member States on the protection of personal data collected and processed for insurance purposes. Here, “actuarial activities” and hence rating, which is essential for the insurance industry, are allowed as well

(recommendations 4.4. k). The same applies to preparing and issuing insurance, i.e. risk-based pricing and premium calculation (recommendations 4.4. a).

According to Art. 44 of the Solvency II Framework Directive (Directive 2009/138/EC), proper business organization of an insurer presupposes adequate risk management. This includes risk assessment and risk identification. The overall risk of the company has to be determined by aggregating individual risks. Within the scope of necessary risk management, risk-based pricing and risk assessment are imperative.

In mass lines of business, rate classification partly also takes place in an automated manner. This trend will continue in the future.

Commission proposal for a Regulation:

Art. 20 of the regulation proposal generally prohibits profiling based on automated processes. This is primarily intended to prevent the creation of behaviour profiles based on activities on the internet. However, according to its wording, the provision would also cover automated rate classification and risk assessment in the insurance industry, thus jeopardizing the essence of the activities of the insurance industry. Actually, however, these are fundamentally different facts. The insurance-specific procedures are precisely not aimed at analysing or predicting personal preferences, behaviour or attitudes of individual persons, but at creating groups with a homogeneous risk situation, so as to be able to provide compensation from the sum of the premiums to an individual insured belonging to this group who accidentally suffers a loss.

An **automated assessment on the basis of health data**, e.g. in the context of travel health insurance to be taken out quickly, would be generally prohibited according to **Art. 20 (3)**, even if the result is only positive for customers. Any such consequence is presumably not intended and is not in the interest of customers, who benefit from cost savings and the more rapid policy issuance process.

Furthermore, this rule conflicts with Art. 9 (1) of the E-Commerce Directive of 8 June 2000 (Directive 2000/31/EC), which reads as follows:

> "Member States shall ensure that their legal system allows contracts to be concluded by electronic means. Member States shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means."

In this respect, the future regulation itself represents an "obstacle for the use of electronic contracts", which is precisely to be promoted by means of the E-Commerce Directive.

Position of the German insurance industry:

Risk-based pricing and risk assessment in the insurance industry should be explicitly excluded from the concept of profiling as referred to in Art. 20.

b) Overly expansive definition of the personal character of data

The overly expansive definition of personal data leads to disproportionate restrictions with respect to the processing of not very sensitive data on objects and of pseudonymized data.

Background:

For risk assessment, the insurance industry also uses not very sensitive data, which are initially not linked to any person.

Example:

> In natural hazards insurance, insurers use the freely accessible risk maps of public authorities. For instance, German water authorities provide information on flood zones, the German Weather Service (*Deutscher Wetterdienst*) holds information available on heavy rain and storm. This is complemented by resolution-restricted air photographs of the Federal Agency for Cartography and Geodesy (*Bundesamt für Kartografie und Geodäsie*). These data are initially not related to any concrete person and in most cases those who forward them are unable to relate them to any specific person.

Commission proposal for a Regulation:

Art. 4 (1) and (2) of the proposal assume a **very wide definition of the personal character** of data. It suffices that any third party – rather than only the controller – could establish the personal character. Thus, the most extensive legal opinion held in literature to define the concept of personal data is used as a basis. Not even the restrictions made by the Article 29 Data Protection Working Party in its Working Paper 136 (Opinion 4/2007) with respect to the concept of 'personal data' dated 20 June 2007 are taken into account.

In this exemplary case, according to the wide definition, a datum which can be related to a person and is hence equated with a personal datum, would exist right from the beginning because there is a possibility that somebody observes that a house is situated in an area where floods are frequent and another person may attribute this house to an owner. Furthermore, objective, not very sensitive data on objects are subject to the same requirements as direct statements on a specific person.

Moreover, since it suffices according to the explicit rule referred to in Art. 4 (1) that somebody may attribute the data to an identification number, any

pseudonymization of data is also irrelevant with this definition under data protection law.

Position of the German insurance industry:

To **prevent the concept of personal data being applied too widely** and hence data protection law from being watered down, it is necessary to **restrict the definition**. **Privileges** should be created **for data on objects which cannot be directly related to a person and for pseudonymized data**.

Restrictions only for completely anonymized data do not suffice. If this rule for the protection of the right to informational self-determination does not suffice for certain cases, these may be regulated separately.

3. Prevention of insurance fraud and ensuring the reliability of intermediaries

The information systems of the insurance industry for protection against insurance fraud and unreliable insurance intermediaries should not be deprived of their legal basis.

Background:

In property, casualty and accident insurance alone, the German insurance industry suffers losses estimated at four billion EUR per year due to insurance fraud.

> A study conducted by the Society for Consumer Research (*Gesellschaft für Konsumforschung - GfK*) in 2011 revealed that approx. four per cent of households interviewed openly admitted to having committed insurance fraud in the last five years. A further seven per cent know of a concrete case of insurance fraud. Special surveys have shown that up to 40 % of claims concerning smartphones, flat screen TVs and laptops were filed with the intent to defraud.

These costs make insurance cover considerably more expensive for honest insurance customers. Therefore, in the interest of insureds, the insurance industry relies on measures to combat fraud. In Germany, for instance, this is the purpose of the **Detection and Information System (*Hinweis- und Informationssystem - HIS*)**, which has been reorganized according to the guidelines set by the German data protection authorities as recently as 2011. In this system, certain data from insurance companies are stored which suggest increased risk. Moreover, in clearly defined cases, there may be a data exchange between insurance companies concerned.

The **Information Office on the Insurance and Buildings Societies' Field Service (*Auskunftsstelle über den Versicherungs- und Bausparaußendienst - AVAD*)** also processes information on intermediaries to ensure their reliability in the interest of consumers. The statutory purpose of AVAD is to achieve the aim that only trustworthy persons act as intermediaries with respect to insurance products, products of building societies and other financial services products. Their activity serves to implement the Insurance Mediation Directive (Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation) in Germany. The identification and naming of dishonest intermediaries is necessary because permanent control of intermediaries is not ensured. Particularly for the area of tied insurance intermediaries, the reliability check is solely made by companies. In this respect, AVAD is an indispensable means of checking as information bureau of the sector. Therefore, AVAD has been recognized both by the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht - BaFin*), i.e. the German insurance supervisory authority, and by the German data protection authorities.

The fraud combating system HIS also stores **convictions due to insurance fraud**, which may be queried by other insurers. AVAD holds data on **criminal convictions** concerning the reliability of insurance intermediaries, too.

Commission proposal for a Regulation:

Contrary to the existing EU Directive on Personal Data Protection, the proposal for an EU Data Protection Regulation **does not provide** for a **clear legal basis** for the operation of information offices. It is uncertain whether Art. 6 (1) (f) is to cover these cases as well because this rule falls short of Art. 7 (f) of Directive 95/46/EC, which also covers **data processing in the interest of third parties**. Thus, the Detection and Information System of the German insurance industry (HIS), which serves to combat insurance fraud and has just been organized as an information bureau at the request of data protection authorities, no longer rests on a secure legal basis. Also, data transfers to the system as well as to other companies, which are currently permitted under clearly defined criteria, become doubtful because Art. 6 (1) (f) of the regulation proposal does not allow any data transfer in the interest of third parties. The same applies to the Information Office on the Insurance and Building Societies' Field Service (AVAD).

Art. 9 (1) and 2 (j) make the processing of data on criminal convictions subject to a declaration of consent – which results in legal insecurity precisely in this case – or to a special national or European law. Such a law does not exist, at least in Germany.

Position of the German insurance industry:

The operation of the systems mentioned should be ensured by allowing data processing in the interest of third parties and by making the processing of data on criminal convictions possible in the case of significant legitimate interest directly on the basis of the regulation.

4. Rights of data subjects

Extensive rights of data subjects should not jeopardize the performance of contracts and the execution of appropriate business processes.

Effective data protection presupposes that data subjects are informed about the processing of their data. However, the rights granted to data subjects by the regulation go far beyond the current data protection level of all Member States. They even exceed the German data protection standard, which is considered to be very high. For companies, extensive notification duties and duties of disclosure as well as the right to be forgotten and the right to data portability not only represent a considerable bureaucratic burden. There is also a risk that necessary and appropriate business processes, which are also in the interest of customers, are impeded or even made impossible. In this context, it should be ensured that rules which are suitable for online social networks are not applied on a one-to-one basis to offline operations.

a) Right to be forgotten and right to erasure

Art. 17 stipulates a comprehensive **right to be forgotten and to erasure**.

Art. 17 (1) provides for numerous reasons which must lead to erasure of data, including withdrawal of consent (Art. 17 (1) (b) or (d)). Since the alternatives referred to in Art. 17 (1) are independent of each other, this applies even during the term of an existing contract. However, it should, for instance, not be possible that a customer wholly or partly withdraws stored data from the insurer, thus making any objective claims assessment impossible, or disengages from the contract prematurely.

Position of the German insurance industry:

The right to be forgotten should be excluded if the data are necessary for the performance of a contract.

b) Blocking instead of erasure

Today's technological systems normally do not allow any complete erasure of data. For instance, no partial files may be eliminated from data which have been backed up photographically on storage disks. Such

methods of storing are used, for instance, in areas where scanned data have to be available in an unalterable manner after destruction of the actual documents. Thus, the obligation to erase the data completely becomes unrealizable. The only possibility is to make any access impossible.

Position of the German insurance industry:

For the case that erasure is impossible for technical reasons, blocking of the data must suffice. This is stipulated, for instance, in Germany according to Sect. 35, para. 3, no. 3 of the Federal Data Protection Act.

c) Right to data portability

A right to data portability according to Art. 18 may arguably be applied appropriately if a person posts his or her **own content** on the **Internet**, such as photographs or texts in online social networks. It is also plausible if persons surrender their own files to a cloud provider for storage. For these Internet applications it should basically be possible to either eliminate this content or transfer it to another provider. However, the scope of Art. 18 goes far beyond these case groups.

In the insurance industry, data are processed in an especially secure manner for the purpose of performing contracts or settling claims. However, since **structured formats** are used as well, **Art. 18 (1)** would require insurance companies to make available copies of the data processed by them in a structured electronic format which the respective person may continue to use. Since data processing systems have been programmed for completely different procedures, this would necessarily involve considerable technical effort and financial expense and would go far beyond the object of the company.

Art. 18 (2) goes even further, being always applicable whenever a person has made his or her data available and the processing is based on consent or a contract. Thus, for instance, most customer data processed by insurers would be concerned by this paragraph. **Transferring the data to other systems** not only involves a great amount of technical effort. It would also be of no benefit to the customer because different tariffs apply with the new insurer whose terms – and therefore potential benefits for the customer – may differ significantly. Furthermore, rate structures and hence business secrets would be apparent from data records, so that this rule may conflict with competition law.

Position of the German insurance industry:

In the insurance industry, which processes data in an especially secure manner to perform contracts or to meet claims, the right to data portability does not make sense.

d) Rights to information and of access

Transparency is an important element of data protection. Therefore, data subjects should know who processes their data and should be able to receive detailed information. The **information requirements** according to Art. 14 and the **duties of disclosure** according to Art. 15 are too extensive and can hardly be fulfilled in practice. The information requirements according to Art. 14 are already so detailed that they will not likely be of interest to many customers. They may be developed further by means of delegated legal acts. Thus, they clearly exceed even German law, which is very strict. In sectors processing a substantial amount of data, like the insurance industry, rights of access may get too extensive if they are not specified. They must be limited to protect secret data.

Position of the German insurance industry:

Data subjects should not be overloaded with extensive information according to Art. 14, but should receive the information they need to exercise their right of access. Requests for access should be specified by the data subject, so that it is possible to reply in a targeted way and unnecessary research effort is avoided.

Rules in German law, namely Sects. 33 and 34 of the Federal Data Protection Act, including the exceptions mentioned there, may serve as a model.

5. Avoiding bureaucratic burdens

Given the fact that data protection standards are high anyway, the requirements for data protection and data security should be stipulated with a sense of proportion, thus avoiding unnecessary bureaucratic burdens.

Contrary to the Commission's declared objective of reducing bureaucracy, the regulation entails considerable new bureaucratic burdens. Throughout the entire regulation proposal, there are requirements for companies which lead to a quite considerable administrative burden. Examples of these include the detailed and extensive provisions on the development and proof of data protection strategies (Art. 22), on the implementation and use of data-protection-friendly technology (Art. 23), on documentation of processing operations (Art. 28), on ensuring data security (Art. 30) and on cooperation with the supervisory authority (Articles 29, 34). These obligations, which are extensive anyway, may usually be further specified by the Commission through delegated legal acts or be formalized through implementing measures.

Only especially far-reaching obligations are dealt with below.

a) Data protection impact assessment according to Art. 33

Given the multitude of already existing obligations, the additional requirement of a data protection impact assessment according to Art. 33 is dispensible.

Overall, the **scope of this rule is unclear**. The question arises as to when a processing operation presents "specific risks to the rights and freedoms of data subjects". The example mentioned in Art. 33 (2) (a) is likely to be understood as meaning that numerous data processing operations in the insurance industry, such as classification under a certain rate, require a data protection impact assessment. According to Art. 33 (2) (b), the entire data processing in personal insurance seems to require a data protection impact assessment where health data of individual persons have been collected. Since the supervisory authority may require an impact assessment for further processing operations (Art. 33 (2) (e), Art. 34 (2) (b)), the scope of this rule is incalculable. The intended **content and scope** of the impact assessment are unclear as well. According to Art. 33 (6), the specification of this is left to the Commission.

The rule mentioned in **Art. 33 (4)** is especially burdensome. According to this rule, the **assessment of data subjects or their representatives** has to be sought. Not only does this lead to a considerable bureaucratic burden, but it also **jeopardizes business secrets**. After all, it is to be assumed that planned procedures will become known to the market counterparty, too. Thus, the proposed wording of Art. 33 represents a disproportionate interference with entrepreneurial freedom.

Position of the German insurance industry:

Since the effects of data processing for data subjects have to be observed anyway within the scope of the other requirements, e.g. Art. 23, Art. 33 is dispensable.

b) Reaction to data breaches (Articles 31 und 32)

Even compared to German law, which goes very far, the obligation to **report data breaches** is very strict. According to Articles 4 (9), 31 and 32, any destruction, any loss, any alteration of or any unauthorized access to personal data already suffices. It neither depends on whether the data deserve specific protection because of their nature nor on the severity and consequences of the incident for data subjects. A scope which is **defined as broadly** gives rise to apprehensions regarding a possible **flood of reports** with supervisory authorities and the fact that data subjects, who are notified time and again also in trivial cases, may become indifferent to them.

Position of the German insurance industry:

Articles 31 and 32 should be restricted to the extent that

- they cover only data which deserve specific protection,
- they cover only unlawful transfer or other unlawful gaining knowledge of data and that
- there is inevitably a risk of severe infringements of the rights or interests deserving protection of data subjects.

Section 42a, which has been inserted into the German Federal Data Protection Act in 2009, may serve as a model.

6. One-stop shop

In the future, according to Art. 51 (2), the supervisory authority of the head office country of a company will be competent for its branches as well. For companies operating on a European scale it is a considerable relief that reports, authorization and documentation obligations will have to be fulfilled only once, i.e. centrally, with the competent data protection authority.

However, the effect of this advantage is limited because most groups are organized in such a way that they have legally independent subsidiaries. Basically, every subsidiary is an independent controller within the meaning of the regulation. Therefore, the supervisory authority competent for them is the respective supervisory authority in the Member State where the subsidiary has its head office. It is doubtful whether Art. 24 may be interpreted as widely as meaning a sole competence of the supervisory authority of the parent company.

Thus, notification obligations, authorization/documentation requirements etc. have to be fulfilled by every subsidiary, i.e. several times. Binding corporate rules according to Art. 43 of the regulation proposal not only have to be submitted for authorization with the competent supervisory authority by the parent company of the group, but also by subsidiaries in other EU Member States with the authorities competent for them. Thus, a considerable bureaucratic burden will continue to exist.

Position of the German insurance industry:

The central competence of the supervisory authority according to 51 (2) should cover not only branches, but also subsidiaries according to the definition in Art. 4 (16) of the regulation proposal.

7. Collective redress

Through Art. 76 (1) in conj. with Art. 75, data protection associations are also entitled to bring forward **collective actions**. However, there is no apparent deficit in terms of law enforcement, which would justify such actions. This applies to data protection law even more than it applies to consumer protection law. In fact, for punishing potential data protection violations, there are – unlike, for instance, for reviewing general terms and conditions – special data protection supervisory authorities, which are granted extensive powers of intervention by the regulation. Every data subject may approach these authorities in a formless manner and free of charge. According to Art. 76 (2) of the regulation proposal, data protection authorities are even to be granted a right to sue.

8. Sanctions

Precisely in light of the extensive requirements and great legal uncertainties described above, the comprehensive sanctions according to Art. 79 seem very far-reaching. In this respect, it would be reasonable to adjust, first of all, those provisions whose violation is sanctioned. The possibility of a warning in the case of a first and non-intentional non-compliance (Art. 79 (3)) should be opened up to large companies as well.

9. Delegated legal acts and implementing acts

A final assessment of the effects of the regulation proposal proves difficult because in numerous passages the proposal includes authorizations granted to the Commission with respect to delegated legal acts according to Art. 86 or implementing acts according to the procedure stipulated in Art. 87. While implementing legal acts may be justified in certain areas due to required adjustments to technological developments, the extensive organizational powers granted to the Commission seem too far-reaching on the whole because they involve considerable legal uncertainty for businesses processing data. According to Art. 290 TFEU, the Commission may be granted the power to adopt non-legislative acts of general application to supplement or amend certain non-essential elements of the legislative act. It cannot be assumed that the multitude of provisions which may be amended are non-essential. Furthermore, the rules of the future regulation must already be sufficiently definite. Precisely in light of the massive regulations on sanctions it should be clearly apparent from the outset to persons responsible how far their obligations reach.

<u>Position of the German insurance industry:</u>

Instead of providing for delegated legal acts, data protection law should be put into concrete terms by means of self-regulation measures in the indi-

vidual sectors. **Already under current German data protection law, the German insurance industry follows this path jointly with the German data protection authorities (see above, preliminary remark).** In this respect, Art. 38 of the regulation proposal choses an appropriate approach. However, the requirements with respect to content should be defined less rigidly so as to ensure wide-spread acceptance and practicability.

Berlin, 16 May 2012

Pseudonymisierung in der EU-Datenschutzverordnung

Die Möglichkeiten der Pseudonymisierung sollten stärker in der Verordnung Platz greifen. Für den verstärkten Einsatz pseudonymisierter Datenverarbeitung sprechen gewichtige Argumente:

- Die pseudonymisierte Datenverarbeitung schafft eine gerechte Balance zwischen Datenschutz des Betroffenen und Interesse des Datenverarbeiters.

- Die EU-Kommission hat in ihrem Verordnungsentwurf bereits erste gute Ansätze entwickelt, wie der Einsatz pseudonymisierter Verfahren aussehen kann. Art. 83 Abs. 1 erlaubt eine Datenverarbeitung unter anderem zu statistischen Zwecken, soweit die Daten anonymisiert oder pseudonymisiert verarbeitet werden. Dieser Ansatz wird jedoch durch den Berichtsentwurf des LIBE zu Art. 81 Abs. 2 in Verbindung mit Art. 83 Abs. 1 konterkariert und zugunsten eines Einwilligungsvorbehalts für Gesundheitsdaten in nicht nachvollziehbarer Weise verdrängt. Die Einwilligung ist aufgrund von Art. 7 Abs. 4 jedoch in höchstem Maß unsicher und impraktikabel.

- Alle mitberatenden Ausschüsse im Europäischen Parlament fordern in zahlreichen Änderungsanträgen eine Privilegierung pseudonymisierter Daten, die am Art. 6 Abs. 1 ansetzen soll. Danach ist die Datenverarbeitung zulässig, wenn (ausschließlich) pseudonymisierte Daten verwendet werden[1].

- Dieser Ansatz ist zu begrüßen und sollte für Gesundheitsdaten weiterentwickelt werden: Soweit sensible Daten pseudonymisiert verarbeitet werden, sollte der Datenverarbeiter dies unter den Voraussetzungen des Art. 6 Abs. 1 Buchstabe a bis f vornehmen dürfen. Diese erhöhten Anforderungen tragen der besonderen Schutzwürdigkeit sensibler Daten Rechnung.

- Es gibt zahlreiche Vertragsbeziehungen, bei denen regelmäßig Datensätze verarbeitet werden, die sowohl nicht sensible (z. B. Name) als auch sensible Daten (z. B. Gesundheitsdaten) enthalten. Dies ist etwa bei Bearbeitung eines Antrages zum Abschluss eines Versicherungsvertrages der Fall. Der Einsatz pseudonymisierter Verfahren wird nur erfolgreich sein, wenn es möglich wird, beide Datentypen unter einem Pseudonym zu verarbeiten. Eine künstliche Aufspaltung von sensiblen und nichtsensiblen Daten kann nicht zielführend sein. Insbesondere Rückversicherer verarbeiten Daten regelmäßig unter Einsatz von Pseudonymen. Als Garant für eine zuverlässige Leistungserbringung der Erstversicherer sind sie auf die Pseudonymisierung von sensiblen Daten angewiesen.

[1] JURI: Änderungsantrag 140, IMCO: Änderungsantrag 198, ITRE: Änderungsanträge 374, 377, 380

Stellungnahme

zum Vorschlag der EU-Datenschutzverordnung

KOM(2012) 11/4

vom 25. Januar 2012

Zusammenfassung

Die Deutsche Versicherungswirtschaft unterstützt die Ziele, das Datenschutzrecht in Europa zu vereinheitlichen, die grenzüberschreitende Tätigkeit zu erleichtern und Hemmnisse für den internationalen Datentransfer zu beseitigen. Die Idee des „One-stop-shops“ sollte ausgebaut werden.

Angesichts des ohnehin schon hohen Datenschutzstandards z. B. in Deutschland sollte eine Regelung der Rechte der Betroffenen und der Anforderungen an Datenschutz und Datensicherheit jedoch mit Augenmaß erfolgen und unnötige bürokratische Belastungen vermeiden. Regelungen, die erkennbar von Vorfällen in der Internetwirtschaft angestoßen sind und nur für den Bereich des Internets Sinn ergeben, sollten dabei nicht generell und allgemeingültig gemacht werden.

Im Hinblick auf versicherungsspezifische Geschäftsabläufe enthält der Vorschlag der Datenschutz-Grundverordnung noch erhebliche rechtliche Unsicherheiten sowie Bestimmungen, die die Bereitstellung von Versicherungsschutz erheblich erschweren, verteuern und in Teilen sogar gefährden würden.

Die zukünftige Verordnung sollte insbesondere folgende Punkte berücksichtigen:

- Es bedarf einer eindeutigen **Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten** in der Lebens-, Kranken-, Unfall- und Haftpflichtversicherung und Rückversicherung. Sie muss auch inzwischen gebräuchliche und sinnvolle **Datenverarbeitungen im Konzern und unter Beteiligung spezialisierter Dienstleister** erfassen (dazu Ziffer 1).

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5290
Fax: +49 30 2020-6290

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +32 2 28247-39

Ansprechpartner:
Dr. Martina Vomhof
Leiterin
Datenschutz/Grundsatzfragen

E-Mail: m.vomhof@gdv.de

www.gdv.de

- Tarifierung und Risikodifferenzierung als Kernbestandteile des Versicherungsgeschäfts müssen möglich bleiben. Die auf das Internet zugeschnittenen Bestimmungen zur **Profilbildung** (Art. 20) dürfen die Tarifeinstufung und Risikoeinschätzung in der Versicherungswirtschaft nicht erfassen. Die **Begriffsbestimmungen** müssen dahingehend überarbeitet werden, dass die Nutzung weniger sensibler Sachdaten und pseudonymisierter Daten möglich bleibt. (dazu Ziffer 2).
- Verfahren zum **Schutz vor Versicherungsbetrug und unzuverlässigen Versicherungsvermittlern** müssen durchführbar bleiben (dazu Ziffer 3).
- Umfangreiche **Betroffenenrechte**, wie das Recht auf Vergessen (Art. 17) und Datenübertragbarkeit (Art. 18), die primär auf soziale Netzwerke im Internet zugeschnitten sind, dürfen die Vertragsdurchführung nicht gefährden (dazu Ziffer 4).
- Die **Anforderungen an Maßnahmen zu Datenschutz und Sicherheit** müssen praktikabel bleiben (dazu Ziffer 5). Die erheblich belastende Datenschutz-Folgenabschätzung (Art. 33) sollte entfallen und die Verpflichtung zur Meldung von Datenpannen auf gravierende Fälle eingeschränkt werden (Art. 31, 32).
- Möglichkeiten zur **kollektiven Rechtsdurchsetzung** sind nicht erforderlich, zumal den Datenschutzaufsichtsbehörden weitgehende Kompetenzen eingeräumt sind (dazu Ziffer 7). **Sanktionen** sollten auf ein verträgliches Maß begrenzt werden (Ziffer 8).
- Die weiten Befugnisse der Europäischen Kommission zum **Erlass von delegierten Rechtsakten** bedeuten Rechtsunsicherheit. Vorzugswürdig ist eine Konkretisierung der Verordnung durch branchenspezifische **Selbstregulierungsmaßnahmen** (dazu Ziffer 9).

Inhaltsübersicht

Vorbemerkung

Als Risikoträger für Unternehmen und private Haushalte erfüllt die Versicherungswirtschaft im Rahmen der gesamten Volkswirtschaft eine essentielle Funktion. Ebenso wie individuelle Eigenvorsorge oder eine staatliche Absicherung zählt die Möglichkeit, sich über einen privaten Versicherungsschutz gegen elementare Lebensrisiken abzusichern, in der sozialen Marktwirtschaft zu den Eckpfeilern der Daseinsvorsorge. Indem die Versicherungswirtschaft private oder öffentliche Risiken übernimmt, schafft sie für Unternehmen und Wirtschaft die Sicherheiten, die notwendig sind, damit sich Initiative und innovatives Unternehmertum überhaupt erst entfalten können. Die Absicherung gegen private Lebensrisiken ermöglicht den Bürgerinnen und Bürgern ein Leben in Freiheit und Sicherheit.

Allein in Deutschland bieten Versicherungsunternehmen mit ca. 450 Millionen Versicherungsverträgen umfassenden Risikoschutz und soziale Sicherheit.

Die deutschen Versicherer sind sich ihrer Verantwortung bewusst, die damit einhergeht, dass sie zur Erfüllung ihrer Aufgaben personenbezogene Daten ihrer Kunden und Antragsteller verarbeiten müssen. Aus diesem Grund erarbeitet der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) zurzeit gemeinsam mit den deutschen Datenschutzbehörden aktuell Verhaltensregeln zum Umgang mit personenbezogenen Daten (Code of Conduct). In engem Zusammenhang mit dieser geplanten Selbstregulierungsmaßnahme steht eine gemeinsam erarbeitete datenschutzrechtliche Einwilligungsklausel für die Lebens- und Krankenversicherung, die seit Januar 2012 von den deutschen Datenschutzbehörden empfohlen wird und auch die nach deutschem Strafrecht geforderte Schweigepflichtentbindung umfasst. Auch der Verbraucherzentrale Bundesverband (vzbv) als wichtigste Interessenvertretung der Verbraucher in Deutschland ist an der Ausarbeitung des Code of Conduct und der Einwilligung beteiligt. Die Versicherungswirtschaft wird damit in Deutschland als erste Branche ein Datenschutzkonzept haben, das von Datenschutzbehörden, Verbraucherschützern und Wirtschaft gemeinsam getragen wird.

Vor diesem Hintergrund begrüßt die deutsche Versicherungswirtschaft das Bestreben der Europäischen Kommission, das Datenschutzrecht in Europa zu vereinheitlichen. Für europaweit tätige Unternehmen bedeutet es eine erhebliche Erleichterung, wenn sie sich nicht mit unterschiedlichen materiellen Datenschutzvorschriften auseinandersetzen müssen.
Anreize zur Implementierung von Codes of Conduct (Art. 38) und Binding Corporate Rules (Art. 43) sind sinnvoll. Jedoch sollten die Anforderungen an den Inhalt nicht zu starr festgelegt werden, um eine breite Akzeptanz und Praktikabilität zu sichern.

Aus Sicht der Versicherungswirtschaft sollte die zukünftige Verordnung insbesondere folgende Punkte berücksichtigen:

1. Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft

a) Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten

Es bedarf einer eindeutigen Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten in der Lebens-, Kranken, Unfall- Haftpflicht- und Rückversicherung.

Hintergrund:

In der Krankenversicherung, in der Lebensversicherung und in der Unfallversicherung werden Gesundheitsdaten zwingend benötigt, um im Einklang mit versicherungsaufsichtsrechtlichen Bestimmungen die zu versichernden Risiken zu prüfen und um Versicherungsfälle abwickeln zu können.

Beispiele:

- Es kann nur festgestellt werden, ob ein Versicherter Anspruch auf eine Berufsunfähigkeitsrente hat, wenn geprüft worden ist, ob er eine Erkrankung hat, aufgrund derer er seinen Beruf nicht mehr ausüben kann.
- Ein Krankenrücktransport aus dem Ausland kann nur organisiert werden, wenn dem Versicherer oder Assisteur, der den Transport organisiert, bekannt ist, welche Erkrankung der Versicherte hat.
- Rückversicherer, die Risiken von den Erstversicherern ganz oder teilweise übernehmen und damit die Erfüllung der Verträge sicherstellen, benötigen Gesundheitsdaten, um zu prüfen, ob sie das Risiko zeichnen können bzw. im Versicherungsfall dafür einstehen müssen.
- Haftpflichtversicherer können Personenschäden nur abwickeln, wenn sie die Gesundheitsdaten der Geschädigten verarbeiten können.

Ziel muss es sein, die für die soziale Absicherung der Bevölkerung notwendige Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft auf eine rechtssichere Grundlage zu stellen. Sie muss den Interessen der Versicherten und Antragsteller Rechnung tragen, zu denen auch effiziente Prozessabläufe im Rahmen von Risikoprüfung und Schadenabwicklung zählen.

Verordnungsvorschlag der Kommission:

Der Vorschlag enthält bisher **keine ausreichende gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft**. Eine solche gesetzliche Grundlage ist für die Versicherungsbranche – auch nach Überzeugung der deutschen Datenschutzbehörden – dringend erforderlich.

Der Vorschlag enthält zwar viele Ansatzpunkte, die eine **gesetzliche Grundlage** für die notwendige Verarbeitung von Gesundheitsdaten bieten könnten. Jedoch reichen sie nicht aus:

- Art. 9 Abs. 2f) regelt die Verarbeitung zur Begründung, Geltendmachung oder Abwehr von Rechtsansprüchen, nicht aber (wie Art. 6 Abs. 1b) zur Begründung und Durchführung von Verträgen.
- Art. 9 Abs. 2g) dürfte vermutlich nicht angewendet werden, wenn Art. 9 Abs. 2h) i. V. m. Art. 81 der Verordnung als spezielle Erlaubnisnormen für die Verarbeitung von Gesundheitsdaten verstanden werden.
- Nach Art. 9 Abs. 2h) ist die Verarbeitung von Gesundheitsdaten zulässig, wenn sie vorbehaltlich der Bedingungen und Garantien des Art. 81 für „*Gesundheitszwecke*" erforderlich ist. Damit ist allenfalls die Krankenversicherung erfasst. Inwiefern dies der Fall ist, ist angesichts der Formulierung des Art. 81 Abs. 1c zudem unsicher.

Die Nutzung von **Einwilligungen** als Rechtsgrundlage kann nur eine Notlösung sein. Sie wird den tatsächlichen Geschäftsabläufen nicht gerecht und führt im Ergebnis zu einer Verschlechterung der Situation der Versicherungsnehmer.

Der Vorschlag geht davon aus, dass die betroffene Person eine völlige Entscheidungsfreiheit hat und ihre **Einwilligung jederzeit widerrufen** kann (Art. 7 Abs. 3 und Erwägungsgrund 32). Wenn die Daten zur Durchführung eines Vertrages verarbeitet werden müssen, kann der Kunde theoretisch zwar auf den Vertragsschluss verzichten. Eine Vertragsdurchführung ohne Verarbeitung der Daten ist aber nicht möglich. Bei der inzwischen üblichen Datenverarbeitung in vorgegebenen automatisierten Prozessen, die der Abwicklung von Millionen von Verträgen dient, ist es auch nicht realistisch, dass einzelne Betroffene die Art und Weise der Verarbeitung beeinflussen können.

Die Zulässigkeit der Einwilligungen in der Versicherungswirtschaft wird zudem durch **Art. 7 Abs. 4** des Verordnungsvorschlags infrage gestellt. Danach ist die **Einwilligung** als Rechtsgrundlage der Datenverarbeitung **ausgeschlossen**, wenn zwischen dem Betroffenen und der verantwortlichen Stelle ein **erhebliches Ungleichgewicht** besteht. Nach Erwägungsgrund 34 ist dies der Fall, wenn ein Abhängigkeitsverhältnis besteht, z. B. in Beschäftigungsverhältnissen. Nach der Einschätzung von Datenschutzbehörden ist es auszuschließen, dass ein solches Ungleichgewicht nicht nur zwischen Arbeitgebern und Arbeitnehmern, sondern auch zwischen Versicherungsunternehmen und ihren Kunden oder Geschädigten angenommen wird. Damit wäre eine Einwilligung ausgeschlossen. Ein genereller Ausschluss der Einwilligung in Art. 7 Abs. 4 schränkt Verbraucher in ihrer Entscheidungsfreiheit ein und steht dem eigentlichen Ziel des Datenschutzes entgegen, den Einzelnen als Herrn über seine Daten zu stärken. Die Versicherungswirtschaft stellt er vor große Schwierigkeiten, ihre Datenverarbeitung zu rechtfertigen.

Position der deutschen Versicherungswirtschaft:

Notwendig ist eine eindeutige, europaweit geltende gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten in allen betroffenen Versicherungssparten, also in der Lebens-, Kranken-, Unfall- und Haftpflichtversicherung sowie bei Rückversicherungen. Eine solche gesetzliche Grundlage muss sich auch auf die unternehmensübergreifende Datenverarbeitung im Konzern sowie die Einschaltung von dritten Personen, wie z. B. ärztlichen Gutachtern und Assistance-Unternehmen, erstrecken (dazu unten 2).

Vorschlag der deutschen Versicherungswirtschaft:

Art. 9 Abs. 2 h) sollte wie folgt gefasst werden:

> ***„die Verarbeitung betrifft Gesundheitsdaten und ist vorbehaltlich der Bedingungen und Garantien des Art. 81 oder Art. 81a ~~für Gesundheitszwecke~~ erforderlich oder“***

Es sollte ein **neuer Art. 81 a Abs. 1** eingefügt werden:

> ***„Die Verarbeitung von Gesundheitsdaten ist zulässig, wenn sie für die Erfüllung eines Versicherungsvertrages einschließlich der Rückversicherung oder eines gesetzlichen Haftungsanspruchs, zur Identifizierung erhöhter Risiken oder zum Schutz vor Versicherungsbetrug durch ein Erst- oder Rückversicherungsunternehmen erforderlich ist.“***

Art. 7 Abs. 4 *muss unbedingt* ***gestrichen*** *werden.*

b) Verarbeitung von Gesundheitsdaten im Konzern und Beteiligung von Dienstleistern

Es bedarf einer Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten im Konzern und Beteiligung von Dienstleistern.

Hintergrund:

Um Synergien zu erzielen und dem Gebot der Wirtschaftlichkeit zu entsprechen, müssen innerhalb von Versicherungsgruppen ebenso wie in anderen Branchen Serviceaufgaben delegiert und zentralisiert oder an kompetente Dienstleister ausgelagert werden.

Beispiele:

- Die Entgegennahme von Schadensmeldungen, die Überwachung der Schadensabwicklung sowie die Steuerung von Gutachtenaufträgen wird

von einem bestimmten Konzernunternehmen oder einem spezialisierten Dienstleister übernommen.

- Ein Unternehmen überträgt die gesamte Risikoprüfung und Schadensbearbeitung für alle Konzerngesellschaften Mitarbeitern der Konzernmutter.
- Erkrankungen werden z. B. in kleineren Gesellschaften immer und bei großen Unternehmen in bestimmten Fällen durch externe Ärzte begutachtet.
- Eine Krankenversorgung im Ausland und Krankenrücktransporte werden durch hierauf spezialisierte Assistance-Gesellschaften durchgeführt.
- Die Versorgung mit medizinischen Hilfsmitteln erfolgt durch Fachbetriebe.

Sowohl diese Maßnahmen als auch die Risikoverlagerung auf Rückversicherer sind nach der Richtlinie 2009/138/EG des Europäischen Parlamentes und des Rates vom 25. November 2009 (betreffend die Aufnahme und Ausübung der Versicherungs- und Rückversicherungstätigkeit – Solvency II) versicherungsaufsichtsrechtlich zulässig.

Vorschlag der Kommission:

Art. 4 Abs. 5 und Art. 24 sind für die Regelung der gemeinsamen Datenverarbeitung nicht hilfreich, weil sie keine eindeutige Ermächtigungsgrundlage für eine Datenweitergabe von einer verantwortlichen Stelle an die andere schaffen. Sobald eine gesamte Aufgabe übertragen wird, liegt nach Auffassung vieler Datenschutzbehörden keine Auftragsdatenverarbeitung vor, sodass Art. 26 nicht eingreift.

Wenn Gesundheitsdaten verarbeitet werden, bedarf es somit grundsätzlich für jede Datenübermittlung einer **Einwilligung** des Betroffenen. Abgesehen von den erheblichen rechtlichen Unsicherheiten einer solchen Einwilligung (dazu oben 1a) und dem damit verbundenen Zeit- und Kostenaufwand erweist sich dieser Weg für alle Veränderungen während der Laufzeit eines Versicherungsvertrages als äußerst unpraktikabel. Nach Abschluss des Vertrages reagiert die Mehrzahl der Betroffenen auf die Bitte zur Abgabe der Erklärung erfahrungsgemäß schlichtweg nicht. Es ist nicht möglich, angesichts notwendiger Veränderungen der Geschäftsprozesse immer wieder jeden einzelnen Versicherungsnehmer erneut um seine Einwilligung zu bitten.

Die Probleme können in der Versicherungswirtschaft nicht einfach gelöst werden, indem Unternehmen zusammengelegt und damit zu einer einheitlichen verantwortlichen Stelle gemacht werden. Denn Versicherungsunternehmen sind gemäß Art. 73 der Richtlinie 2009/138/EG grundsätzlich zur **Spartentrennung** zwischen Lebens- und Nichtlebensversicherung verpflichtet. Diese Versicherungssparten dürfen nur durch verschiedene juristische Personen betrieben werden. In Deutschland gilt das Spartentrennungsgebot zudem für die substitutive Krankenversicherung und für die Leistungsbearbeitung in der Rechtsschutzversicherung. Diese Re-

geln dienen nur der Trennung der Haftungsmassen, haben aber keinen datenschutzrechtlichen Grund.

Position der deutschen Versicherungswirtschaft:

Anstelle einer Einwilligung, die von vielen Betroffenen ohne Reflektion abgegeben wird und daher oft keinen besonderen Schutz bietet, sollten gesetzliche Anforderungen an die Zulässigkeit der Datenübermittlung zwischen Unternehmen einer Versicherungsgruppe, an Rückversicherungsunternehmen und an Dienstleister geschaffen werden. Wenn sichergestellt ist, dass die Daten nur dem ursprünglichen Zweck entsprechend verarbeitet werden, dass die anderen Unternehmen unter Berücksichtigung der Eignung der von ihnen zu Datenschutz und Datensicherheit getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt sind und dazu vertraglich vereinbart wurde, dass der Geheimnis- und Datenschutz bei dem anderen Unternehmen gewährleistet ist, muss auch eine Übermittlung von Gesundheitsdaten zulässig sein.

Mit dieser gesetzlichen Lösung würden alle Betroffenen geschützt, unabhängig davon, ob sie eine Einwilligung erteilen oder nicht.

Vorschlag der deutschen Versicherungswirtschaft:

Es sollte ein **neuer Art. 81 a Abs. 2** eingefügt werden:

> ***„Soweit ein Erst- oder Rückversicherungsunternehmen einem anderen Unternehmen oder Personen im Rahmen von Satz 1 Daten zur Verarbeitung im Auftrag oder zur eigenverantwortlichen Erfüllung von Datenverarbeitungs- oder sonstigen Aufgaben überlässt, ist die Weitergabe und anschließende Verarbeitung dieser Daten zu dem von dem Erst- oder Rückversicherungsunternehmen bestimmten Zweck ohne Einwilligung des Betroffenen unter den nachfolgenden Voraussetzungen zulässig. Die anderen Unternehmen oder Personen sind unter Berücksichtigung der Eignung der von ihnen zu Datenschutz und Datensicherheit getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen und es ist vertraglich zu vereinbaren, dass der Geheimnis- und Datenschutz bei dem anderen Unternehmen oder Personen gewährleistet ist wie bei dem Erst- oder Rückversicherungsunternehmen selbst.“***

c) Verarbeitung von genetischen und biometrischen Daten in der Versicherungswirtschaft

aa) Genetische Daten

Die im Versicherungsgeschäft notwendige Verarbeitung von genetischen Daten im muss auf sicherer Rechtsgrundlage möglich sein.

Hintergrund:

Die deutschen Versicherer verlangen weder vor noch nach Abschluss eines Versicherungsvertrages die Durchführung genetischer Untersuchungen. Auf die Ergebnisse vorhandener genetischer Untersuchungen wird im Rahmen des gesetzlich Zulässigen nur bei Abschluss von Verträgen mit sehr hohen Beitragssummen zurückgegriffen. Möglich bleiben muss jedoch die Anzeige bekannter Vorerkrankungen nach Maßgabe des jeweils geltenden Versicherungsvertragsrechts.

Im Rahmen ärztlicher Diagnosen spielt heute neben konventionellen Untersuchungsmethoden häufig die Auswertung genetischer Daten eine Rolle. Welche Art von Krebserkrankung besteht und wie sie behandelt werden kann, kann z. B. konventionell, aber auch anhand genetischer Untersuchungen festgelegt werden. Die Versicherungswirtschaft benötigt Untersuchungsergebnisse für die Risikoprüfung und Leistungsbearbeitung in der Personenversicherung. Die Nutzung der Daten für die Prüfung einer bestehenden, diagnostizierten Erkrankung darf nicht davon abhängen, welche Untersuchungsmethode ein Arzt zugrunde legt.

Verordnungsvorschlag der Kommission:

Nach Art. 4 Abs. 10 sind „genetische Daten“ Daten jedweder Art zu den ererbten oder während der vorgeburtlichen Entwicklung erworbenen Merkmalen eines Menschen. Dieser Begriff der genetischen Daten ist zu weit. Er erfasst z. B. auch das für jedermann sichtbare Geschlecht. Außerdem werden Behinderungen erfasst, die nicht genetisch bedingt sind, sondern während der Schwangerschaft der Mutter, z. B. durch Sauerstoffmangel, erworben wurden.

Art. 9 Abs. 1 bezieht auch „genetische Daten“ in die besonderen Kategorien personenbezogener Daten ein, ohne jedoch hinreichende Ausnahmen festzulegen.

Position der deutschen Versicherungswirtschaft:

Der Begriff der „genetischen Daten“ in Art. 4 Abs. 10 sollte auf mit Untersuchung der DNA, RNA oder der Chromosomen gewonnenen Daten über genetische Eigenschaften eines Menschen begrenzt werden.
Die Nutzung genetischer Daten für die Prüfung einer bestehenden, diagnostizierten Erkrankung muss aber ebenso möglich sein wie die Nutzung der Ergebnisse konventioneller Untersuchungsmethoden, da nicht beeinflussbar ist, welchen Methoden ein Arzt zugrunde legt. Insofern sollten genetische Daten wie Gesundheitsdaten behandelt werden.

Vorschlag der deutschen Versicherungswirtschaft:

Art. 4 Abs. 10 sollte wie folgt neu gefasst werden:

> ***„Genetische Daten sind die durch eine Untersuchung der DNA, RNA oder der Chromosomen gewonnenen Daten über genetische Eigenschaften eines Menschen. Genetische Daten sind wie Gesundheitsdaten zu behandeln.“***

bb) Biometrische Rechnungsgrundlagen

Der Begriff der biometrischen Daten muss klar auf „biometrische Erkennungsdaten“ begrenzt werden.

In der Versicherungsmedizin spielen sogenannte „biometrische Rechnungsgrundlagen“ eine Rolle, d. h. physische oder physiologische Merkmale werden in die versicherungsmathematischen Berechnungen einbezogen. Dies dürfte in Art. 4 Abs. 11 hier nicht gemeint sein. Es könnte jedoch zu Verwechslungen mit den gemeinten biometrische Erkennungsdaten kommen.

Vorschlag der deutschen Versicherungswirtschaft:

> ***In Art. 4 Abs. 11 sollte der Begriff „biometrische Erkennungsdaten“ verwendet werden.***

2. Tarifeinstufung und die Risikoeinschätzung in der Versicherungswirtschaft

a) Abgrenzung von der Profilbildung

Tarifierung und Risikoeinschätzung in der Versicherungswirtschaft müssen klar vom Begriff der Profilbildung in Art. 20 ausgenommen werden.

Hintergrund:

Es entspricht der Natur von Versicherungsverträgen, dass nach bestimmten Kriterien Risikogemeinschaften gebildet werden müssen. Dies geschieht in der Regel aufgrund der statistischen Auswertung bekannter Schadensfälle. Diese werden nach gemeinsamen Merkmalen zusammengefasst und lassen so den statistisch wahrscheinlichen Schadenverlauf der Merkmalsgruppe erkennen. Ein Beispiel dafür sind die in der Versicherungswirtschaft verwendeten Sterbetafeln. Die Wahrscheinlichkeit des Eintritts eines Versicherungsfalls und dessen Ausmaß werden im Einzelfall durch eine Risikoprüfung auf Grundlage der Angaben des Versicherungsnehmers mithilfe der Unternehmensstatistiken sowie weiterer bekannter Wahrscheinlichkeiten, wie medizinischer Erfahrungswerte, bewertet. Der Preis für den Versicherungsschutz wird dann entsprechend der Einordnung festgelegt.

Beispiele:

- In der Elementarschadenversicherung können Häuser, die in einem in regelmäßigen Abständen von Überschwemmungen betroffenen Ort liegen, nicht zu gleichen Konditionen versichert werden wie Häuser, die in einem Ort fernab von Gewässern liegen.
- Ebenso unterscheidet sich die Bemessung eines Beitrags danach, ob ein zu versicherndes Haus ein leicht brennbares Reetdach oder ein feuerfestes Schindeldach hat.
- Ein Hobbypilot kann nicht zu gleichen Bedingungen versichert werden, wie jemand, der kein gefährliches Hobby hat.
- Ein Mensch, der ein schweres Rückenleiden hat, kann in der Berufsunfähigkeitsversicherung nur zu ungünstigeren Bedingungen versichert werden, weil mit höherer Wahrscheinlichkeit Kosten auf die Versichertengemeinschaft zukommen.

Die Datenverarbeitung in der Versicherungswirtschaft wird ausführlich in der Empfehlung des Ministerkomitees des Europarates Rec (2002) 9 an die Mitgliedstaaten über den Schutz von zu Versicherungszwecken erhobenen und verarbeiteten personenbezogenen Daten geregelt. Hier werden auch „aktuarische Aktivitäten“ und damit auch die für die Versicherungswirtschaft wesensnotwendige Tarifierung erlaubt (Empfehlungen 4.4. k). Das Gleiche gilt für die Vorbereitung und den Abschluss der Versicherung, also Tarifeinstufung und Prämienbemessung (Empfehlungen 4.4. a).

Eine ordnungsgemäße Geschäftsorganisation eines Versicherers setzt nach Art. 44 der Solvency II-Rahmenrichtlinie (RL 2009/138/EG) ein angemessenes Risikomanagement voraus. Hierzu gehören auch die Risikoprüfung und -erkennung. Das Gesamtrisiko des Unternehmens ist aus der Aggregation der Einzelrisiken zu ermitteln. Im Rahmen der erforderlichen Risikosteuerung ist die Tarifierung und Risikoeinschätzung zwingend erforderlich.

Die Tarifeinstufung erfolgt in Massensparten teilweise auch automatisiert.
Dieser Trend wird sich in der Zukunft fortsetzen.

Verordnungsvorschlag der Kommission:

Der Vorschlag verbietet in Art. 20 grundsätzlich Profilbildungen aufgrund automatisierter Prozesse. Damit soll in erster Linie die Bildung von Verhaltensprofilen aufgrund von Aktivitäten im Internet verhindert werden. Die Bestimmung würde nach ihrem Wortlaut jedoch auch automatisierte Tarifeinstufungen und Risikoeinschätzungen in der Versicherungswirtschaft erfassen und damit die Arbeit der Versicherungswirtschaft im Kern gefährden. Tatsächlich handelt es sich jedoch um grundlegend andere Sachverhalte. Bei den versicherungstypischen Verfahrensweisen geht es gerade nicht darum, persönliche Präferenzen, Verhaltensweisen oder Einstellungen Einzelner zu analysieren oder vorherzusagen, sondern Gruppen mit gleichartigem Risikobild aufzustellen, um einem einzelnen Versicherten der Gruppe, den zufällig der Versicherungsfall trifft, aus der Summe der Beiträge Ersatz leisten zu können.

Eine **automatisierte Einschätzung aufgrund von Gesundheitsdaten**, z. B. in einer schnell abzuschließenden Reisekrankenversicherung, wäre nach **Art. 20 Abs. 3** generell verboten, selbst wenn das Ergebnis für die Kunden nur positiv ist. Eine solche Konsequenz ist vermutlich nicht gewollt und liegt nicht im Interesse der Kunden, denen die Kostenersparnis und der schnellere Policierungsprozess zugutekommen.

Die Regelung widerspricht auch Art. 9 Abs.1 der E-Commerce-Richtlinie vom 08.06.2000 (RL 2000/31/EG), in der es heißt:

> „Die Mitgliedstaaten stellen sicher, dass ihr Rechtssystem den Abschluss von Verträgen auf elektronischem Wege ermöglicht. Die Mitgliedstaaten stellen insbesondere sicher, dass ihre für den Vertragsabschluss geltenden Rechtsvorschriften weder Hindernisse für die Verwendung elektronischer Verträge bilden noch dazu führen, dass diese Verträge aufgrund des Umstandes, dass sie auf elektronischem Wege zustande gekommen sind, keine rechtliche Wirksamkeit oder Gültigkeit haben."

Die zukünftige Verordnung selbst stellt in diesem Punkt ein „Hindernis für die Verwendung elektronischer Verträge" dar, die durch die E-Commerce-Richtlinie gerade gefördert werden soll.

Position der deutschen Versicherungswirtschaft:

Tarifierung und Risikoeinschätzung in der Versicherungswirtschaft müssen ausdrücklich vom Begriff der Profilbildung in Art. 20 ausgenommen werden.

b) Zu weite Definition der Personenbeziehbarkeit von Daten

Die zu weite Definition personenbezogener Daten führt zu unverhältnismäßigen Einschränkungen bei der Verarbeitung wenig sensibler Sachdaten und pseudonymisierter Daten.

Hintergrund:

Zur Risikoeinschätzung nutzt die Versicherungswirtschaft auch wenig sensible Daten, die zunächst keiner Person zugeordnet sind.

Beispiel:

> In der Naturgefahrenversicherung ziehen Versicherer die frei zugänglichen Gefahrenkarten der öffentlichen Hand heran. So stellen etwa die deutschen Wasserwirtschaftsämter Informationen zu Überschwemmungsgebieten zur Verfügung, der Deutsche Wetterdienst hält Informationen zu Starkregen und Sturm vor. Hinzu kommen auflösungsbeschränkte Luftbilder des Bundesamtes für Kartografie und Geodäsie. Diese Daten sind zunächst nicht auf eine konkrete Person bezogen und von denjenigen, die sie weiterleiten, zumeist auch nicht auf eine bestimmte Person beziehbar.

Verordnungsvorschlag der Kommission:

Der Vorschlag geht in **Art. 4 Abs. 1 und 2** von einem **sehr weiten Begriff der Personenbeziehbarkeit** von Daten aus. Es genügt, dass irgendein Dritter – und nicht nur der für die Verarbeitung Verantwortliche – den Personenbezug herstellen könnte. Zum Begriff der personenbezogenen Daten wird damit die weiteste in der Literatur vertretende Rechtsmeinung zugrunde gelegt. Nicht einmal die Einschränkungen, die die Artikel 29-Datenschutzgruppe in ihrem Working Paper 136 (Stellungnahme 4/2007) zum Begriff „personenbezogene Daten“ vom 20. Juni 2007 gemacht hat, werden berücksichtigt.

Nach der weiten Definition läge in dem Beispielsfall bereits von Anfang an ein personenbeziehbares, also dem personenbezogenen gleichgestelltes Datum vor, weil die Möglichkeit besteht, dass jemand feststellt, dass ein Haus in einem Gebiet liegt, in dem Überschwemmungen häufig sind, und ein anderer dieses Haus einem Eigentümer zuordnen kann. Außerdem gelten für objektive, wenig sensible Sachdaten die gleichen Anforderungen wie für direkte Aussagen zu einer Person.

Da es nach der ausdrücklichen Regelung des Art. 4 Abs. 1 ausreicht, dass irgendjemand die Daten zu einer Kennnummer zuordnen kann, ist mit der Begriffsbestimmung außerdem auch jede Pseudonymisierung von Daten datenschutzrechtlich irrelevant.

Position der deutschen Versicherungswirtschaft:

Um ein **Ausufern des Begriffs der personenbezogenen Daten** und damit eine Verwässerung des Datenschutzrechts zu **vermeiden**, ist es erforderlich, die **Definition einzuschränken**. Es müssen **Privilegierungen für nicht unmittelbar personenbeziehbare Sachdaten sowie pseudonymisierte Daten** geschaffen werden.

Einschränkungen nur für vollständig anonymisierte Daten reichen nicht aus. Sofern für bestimmte Fälle diese Regelung zum Schutz des informationellen Selbstbestimmungsrechts nicht ausreicht, können diese gesondert geregelt werden.

Vorschlag der deutschen Versicherungswirtschaft:

Art. 4 Abs. 1 sollte wie folgt gefasst werden:

„'betroffene Person' eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt mit Mitteln bestimmt werden kann, die der für die Verarbeitung Verantwortliche ~~oder jede sonstige natürliche oder juristische Person~~ nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde, … "

3. Verhinderung von Versicherungsbetrug und Gewährleistung der Zuverlässigkeit von Versicherungsvermittlern

Den Auskunftssystemen der Versicherungswirtschaft zum Schutz vor Versicherungsbetrug und unzuverlässigen Versicherungsvermittlern darf die Rechtsgrundlage nicht entzogen werden.

Hintergrund:

Der deutschen Versicherungswirtschaft entstehen allein in der Schaden- und Unfallversicherung durch Versicherungsbetrug Verluste in einer geschätzten Höhe von vier Milliarden Euro pro Jahr.

> Eine Studie der Gesellschaft für Konsumforschung (GfK) aus dem Jahr 2011 ergab, dass ca. vier Prozent der befragten Haushalte offen zugaben, in den letzten fünf Jahren Versicherungsbetrug begangen zu haben. Weitere ca. sieben Prozent wissen von einem konkreten Versicherungsbetrug. Sonderuntersuchungen haben gezeigt, dass bis zu 40 % der Schäden an Smartphones, Flat-TV's und Laptops in Betrugsabsicht eingereicht wurden.

Diese Kosten verteuern den Versicherungsschutz für redliche Versicherungskunden erheblich. Die Versicherungswirtschaft ist daher im Interesse der Versicherten auf Maßnahmen der Betrugsbekämpfung angewiesen. Dem dient z. B. in Deutschland das **Hinweis- und Informationssystem (HIS)**, das erst im Jahr 2011 nach den Vorgaben der deutschen Datenschutzbehörden neu organisiert wurde. In diesem System werden bestimmte, auf ein erhöhtes Risiko hindeutende Daten aus den Versicherungsunternehmen gespeichert. Darüber hinaus kann es in klar definierten Fällen zu einem Datenaustausch zwischen betroffenen Versicherungsunternehmen kommen.

Auch die **Auskunftsstelle über den Versicherungs- und Bausparaußendienst (AVAD)** verarbeitet Informationen über Vermittler, um im Interesse der Verbraucher deren Zuverlässigkeit sicherzustellen. Satzungsmäßiger Zweck der AVAD ist es, zu erreichen, dass nur vertrauenswürdige Personen Versicherungs-, Bauspar- und sonstige Finanzdienstleistungsprodukte vermitteln. Ihre Tätigkeit dient der Umsetzung der Versicherungsvermittlerrichtlinie (Richtlinie 2002/92/EG des Europäischen Parlaments und des Rates vom 9. Dezember 2002 über Versicherungsvermittlung) in Deutschland. Die Identifizierung und Benennung unlauterer Vermittler ist notwendig, da keine laufende Kontrolle der Vermittler gewährleistet ist. Insbesondere für den Bereich der gebundenen Vermittler findet die Zuverlässigkeitsüberprüfung allein durch die Unternehmen statt. Hier ist die AVAD als Branchenauskunftei ein unverzichtbares Mittel der Überprüfung. Die AVAD ist daher sowohl von der Bundesanstalt für Finanzdienstleistungsaufsicht, also der deutschen Versicherungsaufsichtsbehörde als auch von den deutschen Datenschutzbehörden anerkannt.

In dem Betrugsbekämpfungssystem HIS werden auch **Verurteilungen wegen Versicherungsbetrugs** gespeichert und können von anderen Versicherern abgefragt werden. Die AVAD speichert ebenfalls **Strafurteile**, die sich auf die Zuverlässigkeit von Versicherungsvermittlern beziehen.

<u>Verordnungsvorschlag der Kommission:</u>

Für den Betrieb von Auskunfteien gibt es in dem Vorschlag für dieEU-Datenschutzgrundverordnung **keine klare gesetzliche Grundlage** mehr. Ob Art. 6 Abs. 1f. auch diese Fälle erfassen soll, ist unsicher, weil die Norm hinter Art. 7f) der RL 95/46/EG, der auch eine **Datenverarbeitung im Interesse Dritter** erfasst, zurückbleibt. Damit steht das Hinweis- und Informationssystem (HIS) der deutschen Versicherungswirtschaft, das der Bekämpfung von Versicherungsbetrug dient und auf Wunsch der Datenschutzbehörden gerade erst als Auskunftei ausgestaltet wurde, auf keiner sicheren Rechtsgrundlage mehr. Auch Datenübermittlungen an das System sowie an andere Unternehmen, die heute nach klar umschriebenen Kriterien erlaubt sind, werden zweifelhaft, weil Art. 6 Abs. 1f. des Verordnungsvorschlags keine Datenübermittlung im Interesse Dritter zulässt.

Entsprechendes gilt für die Auskunftsstelle über den Versicherungs- und Bausparaußendienst (AVAD).
Durch Art. 9 Abs. 1, 2 (j) wird die Verarbeitung von Daten über Strafurteile an eine rechtlich gerade in diesem Fall sehr unsichere Einwilligung oder ein spezielles nationales oder europäisches Gesetz geknüpft. Ein solches Gesetz liegt zumindest in Deutschland nicht vor.

Position der deutschen Versicherungswirtschaft:

Der Betrieb der genannten Systeme muss sichergestellt werden, indem eine Datenverarbeitung im Interesse Dritter zugelassen wird sowie eine Verarbeitung von Daten über Strafurteile bei erheblichem berechtigten Interesse unmittelbar aufgrund der Verordnung ermöglicht wird.

Vorschlag der deutschen Versicherungswirtschaft:

Art. 6 Abs. 1 f) Satz 1 sollte wie folgt gefasst werden:

> ***„Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.“***

Art. 9 Abs. 2 j) sollte wie folgt gefasst werden:

> ***„die Verarbeitung von Daten über Strafurteile oder damit zusammenhängende Sicherungsmaßregeln erfolgt entweder unter behördlicher Aufsicht oder aufgrund einer gesetzlichen oder rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt, oder zur Wahrnehmung eines wichtigen öffentlichen Interesses oder sonstigen erheblichen berechtigten Interesses, das die schutzwürdigen Interessen der Betroffenen deutlich überwiegt. Ein vollständiges Strafregister darf nur unter behördlicher Aufsicht geführt werden.“***

4. Betroffenenrechte

Umfangreiche Betroffenenrechte dürfen die Vertragsdurchführung und die Durchführung sinnvoller Geschäftsprozesse nicht gefährden.

Ein effektiver Datenschutz setzt voraus, dass die Betroffenen über die Verarbeitung ihrer Daten informiert sind. Jedoch gehen die Rechte, die den Betroffenen durch die Verordnung eingeräumt werden, weit über das aktuelle Datenschutzniveau aller Mitgliedstaaten hinaus. Sie übersteigen sogar den als besonders hoch geltenden deutschen Datenschutzstandard.

Für die Unternehmen bedeuten umfangreiche Benachrichtigungs- und Auskunftspflichten sowie die Rechte auf Vergessenwerden und auf Datenübertragbarkeit nicht nur erheblichen Bürokratieaufwand. Es besteht auch die Gefahr, dass notwendige und sinnvolle Geschäftsabläufe, die auch im Interesse der Kunden liegen, behindert oder sogar unmöglich gemacht werden. Es muss dabei darauf geachtet werden, dass Regelungen, die für soziale Online-Netzwerke passend sind, nicht 1:1 auf den Offline-Betrieb übertragen werden.

a) Recht auf Vergessenwerden und Löschung

In Art. 17 wird ein umfangreiches **Recht auf Vergessenwerden und Löschung** geregelt.

Art. 17 sieht in Absatz 1 zahlreiche Gründe vor, die zur Löschung der Daten führen müssen, u. a. auch den Widerruf einer Einwilligung (Art. 17 Abs. 1b) bzw. d). Da die Alternativen des Art. 17 Abs. 1 nebeneinanderstehen, gilt dies selbst während eines laufenden Vertrages. Jedoch darf es z. B. nicht möglich sein, dass ein Kunde dem Versicherer den Datenbestand ganz oder zum Teil entzieht und damit eine sachliche Leistungsprüfung unmöglich macht oder sich vorzeitig vom Vertrag löst.

Position der deutschen Versicherungswirtschaft:

Das Recht auf Vergessenwerden muss ausgeschlossen sein, wenn die Daten zur Durchführung eines Vertrages erforderlich sind.

Vorschlag der deutschen Versicherungswirtschaft:

In Art. 17 Abs. 3 sollte am Ende ein neuer Buchstabe e eingefügt werden (Buchstabe e wird Buchstabe f):

> ***„für die Durchführung eines Vertrages oder die Erfüllung gesetzlicher Ansprüche.“***

b) Sperrung statt Löschung

Die heutigen technischen Systeme ermöglichen in aller Regel keine vollständige Löschung der Daten. So lassen sich etwa aus auf Speicherplatten fotografisch gesicherten Daten keine Teildateien entfernen. Derartige Speichermethoden werden z. B. in Bereichen verwendet, in denen eingescannte Daten nach Vernichtung der Dokumente unveränderbar zur Verfügung stehen müssen. Die Verpflichtung zur vollständigen Löschung wird damit unerfüllbar. Es kann lediglich der Zugriff unmöglich gemacht werden.

Position der deutschen Versicherungswirtschaft:

Für diesen Fall, dass eine Löschung aus technischen Gründen nicht möglich ist, muss eine Sperrung der Daten ausreichen, wie es z. B. in Deutschland in § 35 Abs. 3 Nr. 3 BDSG vorgesehen ist.

Vorschlag der deutschen Versicherungswirtschaft:

In Art. 17 Abs. 4 wird am Ende eingefügt:

> ***„e) eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.“***

c) Recht auf Datenübertragbarkeit

Ein Recht auf Datenübertragbarkeit nach Art. 18 kann wohl dann sinnvoll angewendet werden, wenn eine Person **eigene Inhalte** in das **Internet** stellt, wie z. B. Fotos oder Texte in sozialen Online-Netzwerken. Es ist auch dann nachvollziehbar, wenn Personen eigene Dateien einem Cloud-Anbieter zur Speicherung überlassen. Bei diesen Internet-Anwendungen muss es grundsätzlich möglich sein, die Inhalte wieder zu entfernen oder einem anderen Anbieter zu übertragen. Jedoch geht der Anwendungsbereich des Art. 18 weit über diese Fallgruppen hinaus.

In der Versicherungswirtschaft werden die Daten gesichert zu Zwecken der Vertragsdurchführung oder Abwicklung von Ansprüchen verarbeitet. Da jedoch auch **strukturierte Formate** verwendet werden, müssten Versicherungsunternehmen nach **Art. 18 Abs. 1** Kopien der von ihnen verarbeiteten Daten in einem für die jeweilige Person weiterverwendbaren strukturierten elektronischen Format zur Verfügung stellen. Da die Datenverarbeitungssysteme für völlig andere Abläufe programmiert sind, wäre das nur mit erheblichem technischen und finanziellen Aufwand möglich und ginge über den Unternehmenszweck weit hinaus.

Noch weiter geht **Art. 18 Abs. 2**, der immer eingreift, wenn eine Person ihre Daten zur Verfügung gestellt hat und die Verarbeitung auf einer Einwilligung oder einem Vertrag basiert. Damit fielen z. B. die meisten Kundendaten darunter, die Versicherer verarbeiten. Eine **Überführung der Daten in andere Systeme** ist nicht nur technisch aufwendig. Sie würde auch für den Kunden keinen Nutzen generieren, da beim neuen Versicherer andere Tarife gelten. Zudem wären aus den Datensätzen Tarifstrukturen und damit Geschäftsgeheimnisse erkennbar, sodass auch erhebliche wettbewerbsrechtliche Bedenken bestehen.

Position der deutschen Versicherungswirtschaft:

In der Versicherungswirtschaft, die die Daten zur Durchführung von Verträgen oder zur Erfüllung von Ansprüchen gesichert verarbeitet, ergibt das Recht auf Datenübertragbarkeit keinen Sinn.

Vorschlag der deutschen Versicherungswirtschaft:

> ***Art. 18 Abs. 1 und 2 müssen auf die Fälle begrenzt werden, in denen die Betroffenen eigene Inhalte in das Internet eingestellt haben.***

d) Informations- und Auskunftsrechte

Transparenz ist ein wichtiges Element des Datenschutzes. Die Betroffenen sollten daher wissen, wer ihre Daten verarbeitet und im Detail Auskunft erhalten können. Zu umfangreich und praktisch kaum erfüllbar sind die **Informationspflichten** aus Art. 14 und die **Auskunftspflichten** aus Art. 15. Die Informationspflichten nach Art. 14 haben bereits eine Detailtiefe, die für viele Kunden nicht von Interesse sein dürfte. Sie können durch delegierte Rechtsakte noch weiter ausgestaltet werden. Damit gehen sie selbst über das scharfe deutsche Recht deutlich hinaus. Auskunftsrechte können in Branchen, die wie die Versicherungswirtschaft umfangreiche Daten verarbeiten, uferlos werden, wenn sie nicht spezifiziert werden. Sie müssen dort an ihrer Grenzen stoßen, wo Tatsachen geheimhaltungsbedürftig sind.

Position der deutschen Versicherungswirtschaft:

Den Betroffenen sollten mit Art. 14 nicht umfangreiche Informationen aufgedrängt werden, sondern sie sollten die Informationen erhalten, die sie benötigen, um ihr Auskunftsrecht wahrzunehmen. Auskunftswünsche sollten vom Betroffenen spezifiziert werden, um zielgerichtet antworten zu können und unnötigen Rechercheaufwand zu vermeiden.

Ein Vorbild können die Regelungen im deutschen Recht, §§ 33 und 34 BDSG einschließlich der dort genannten Ausnahmen sein.

5. Vermeidung bürokratischer Belastungen

Im Hinblick auf den ohnehin schon hohen Datenschutzstandard sollte die Regelung der Anforderungen an Datenschutz und Datensicherheit mit Augenmaß erfolgen und unnötige bürokratische Belastungen vermeiden.

Entgegen dem erklärten Ziel der Kommission, Bürokratie abzubauen, bringt die Verordnung erhebliche neue bürokratische Belastungen mit sich. Durch den gesamten Verordnungsvorschlag ziehen sich Anforderungen an die Unternehmen, die ganz erheblichen Verwaltungsaufwand zur Folge haben. Nur bespielhaft genannt seien die detaillierten und umfangreichen Vorschriften zur Erstellung und zum Nachweis von Datenschutzstrategien (Art. 22), zur Implementierung und zum Einsatz datenschutzfreundlicher Technik (Art. 23), zur Dokumentation der Verarbeitungsvorgänge (Art. 28), zur Gewährleistung der Datensicherheit (Art. 30) und zur Zusammenarbeit mit der Aufsichtsbehörde (Art. 29, 34). Diese ohnehin schon umfangreichen Pflichten können in aller Regel von der Kommission noch durch delegierte Rechtsakte weiter konkretisiert oder durch Durchführungsbestimmungen formalisiert werden.

Nachfolgend wird nur auf die besonders einschneidenden Pflichten eingegangen.

a) Datenschutzfolgeabschätzung nach Art. 33

Angesichts der Vielzahl von Verpflichtungen, die bereits bestehen, ist das zusätzliche Erfordernis einer Datenschutzfolgeabschätzung nach Art. 33 nicht nachvollziehbar.

Bereits der **Anwendungsbereich der Norm ist nicht eindeutig**. So stellt sich die Frage, wann ein Verarbeitungsvorgang „konkrete Risiken“ für die Rechte und Freiheiten betroffener Personen“ birgt. Das Regelbeispiel des Art. 33 Abs. 2a) dürfte so zu verstehen sein, dass zahlreiche Datenverarbeitungen in der Versicherungswirtschaft, wie z. B. die Einstufung in einen Tarif, eine Datenschutzfolgeabschätzung erfordern. Nach Art. 33 Abs. 2 b) scheint die gesamte Datenverarbeitung in der Personenversicherung der Datenschutzfolgeabschätzung zu bedürfen, wenn Gesundheitsdaten von Einzelpersonen erfasst sind. Da die Aufsichtsbehörde für weitere Verarbeitungsvorgänge eine Folgenabschätzung verlangen kann (Art. 33 Abs. 2e), Art. 34 Abs. 2b)), ist der Anwendungsbereich der Regelung unabsehbar. Auch ist nicht klar, welchen **Inhalt und Umfang** die Folgenabschätzung haben soll. Die nähere Bestimmung ist nach Art. 33 Abs. 6 der Kommission überlassen.

Besonders belastend ist die Regelung des **Art. 33 Abs. 4**. Danach muss die **Einschätzung der Betroffenen oder ihrer Repräsentanten** eingeholt werden. Dies führt nicht nur zu erheblichem Bürokratieaufwand, sondern **gefährdet Geschäftsgeheimnisse**. Schließlich ist anzunehmen, dass auf diesem Weg auch der Marktgegenseite geplante Verfahren bekannt werden. Art. 33 in der vorgeschlagenen Fassung stellt damit einen unverhältnismäßigen Eingriff in die unternehmerische Freiheit dar.

Position der deutschen Versicherungswirtschaft:

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.

Vorschlag der deutschen Versicherungswirtschaft:

Art. 33 wird gestrichen.

b) Reaktion auf Datenpannen (Art. 31 und 32)

Die Verpflichtung zur **Meldung von Datenpannen** wird sogar im Vergleich zu dem sehr weitgehenden deutschen Recht sehr strikt ausgestaltet. Nach Art. 4 Abs. 9, 31, 32 genügt bereits jede Zerstörung, jeder Verlust, jede Veränderung oder jeder unberechtigte Zugriff auf personenbezogene Daten. Es kommt weder darauf an, ob die Daten ihrer Art nach besonders schutzwürdig sind noch auf die Schwere und Tragweite des Vorfalls für die Betroffenen. Ein so **weit gefasster Anwendungsbereich** lässt eine **Meldeflut** bei den Aufsichtsbehörden und eine Abstumpfung der immer wieder auch in nichtigen Fällen benachrichtigten Betroffenen befürchten.

Position der deutschen Versicherungswirtschaft:

Art. 31 und 32 sollten 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.

6. One stop-shop

Künftig ist nach Art. 51 Abs. 2 die Aufsichtsbehörde am Hauptsitz eines Unternehmens auch für dessen Zweigniederlassungen zuständig. Für europaweit tätige Unternehmen bedeutet es eine erhebliche Erleichterung, dass Meldungen, Genehmigungs- und Dokumentationserfordernisse nur noch einmal zentral bei der zuständigen Datenschutzbehörde erfolgen müssen.

Allerdings ist dieser Vorteil nur begrenzt, weil die meisten Konzerne so organisiert sind, dass sie rechtlich selbständige Tochtergesellschaften haben. Jede Tochtergesellschaft ist grundsätzlich eine eigene verantwortliche Stelle im Sinne der Verordnung. Für sie ist daher jeweils die Aufsichtsbehörde in dem Mitgliedstaat zuständig, in dem die Tochtergesellschaft ihren Sitz hat. Ob Art. 24 so weit ausgelegt werden kann, dass eine Zuständigkeit nur der Aufsichtsbehörde der Muttergesellschaft begründet werden kann, ist zweifelhaft.

Meldepflichten, Genehmigungs-/ Dokumentationserfordernisse etc. fallen also jeweils pro Tochtergesellschaft und damit mehrfach an. Binding Corporate Rules nach Art. 43 des Verordnungsvorschlags müssen nicht nur von der Konzernmutter zur Genehmigung bei der zuständigen Aufsichtsbehörde eingereicht werden, sondern auch von Tochtergesellschaften in anderen EU-Mitgliedstaaten bei den für sie zuständigen Behörden. Damit bleibt es bei erheblichem Bürokratieaufwand.

Vorschlag der deutschen Versicherungswirtschaft:

Die zentrale Zuständigkeit der Aufsichtsbehörde nach Art. 51 Abs. 2 sollte nicht nur Niederlassungen, sondern auch Konzerntöchter entsprechend der Definition in Art. 4 Abs. 16 des Verordnungsentwurfs erfassen.

7. Kollektive Rechtsdurchsetzung

Über Art. 76 Abs. 1 i. V. m. Art. 75 werden Datenschutzverbände auch zu **Sammelklagen** berechtigt. Es ist jedoch kein Rechtsdurchsetzungsdefizit erkennbar, das derartige Klagen rechtfertigt. Das gilt im Datenschutzrecht noch mehr als im Verbraucherschutzrecht. Zur Ahndung möglicher Datenschutzverstöße gibt es hier nämlich – anders als z. B. bei der Überprüfung von AGB – spezielle Datenschutzaufsichtsbehörden, die nach der Verordnung umfangreiche Eingriffsbefugnisse haben. Jeder Betroffene kann sich form- und kostenlos an die Behörden wenden. Nach dem Verordnungsvorschlag soll den Datenschutzbehörden in Art. 76 Abs. 2 sogar eine Klagebefugnis verliehen werden.

Vorschlag der deutschen Versicherungswirtschaft:

Art. 76 Abs. 1 sollte gestrichen werden.

8. Sanktionen

Gerade angesichts der oben geschilderten umfangreichen Anforderungen und der hohen Rechtsunsicherheiten escheinen die umfangreichen Sank-

tionen in Art. 79 sehr einschneidend. Hier sollten aber zunächst die Vorschriften angepasst werden, deren Verletzung sanktioniert wird. Auch für große Unternehmen sollte die Möglichkeit der Verwarnung bei ersten unbeabsichtigten Verstößen (Art. 79 Abs. 3) eröffnet werden.

Vorschlag der deutschen Versicherungswirtschaft:

Art. 79 Abs. 3 sollte wie folgt gefasst werden:

> ***„Handelt es sich um einen ersten, unabsichtlichen Verstoß gegen diese Verordnung, kann anstatt einer Sanktion eine schriftliche Verwarnung erfolgen."***

9. Delegierte Rechtsakte und Durchführungsakte

Eine abschließende Einschätzung der Auswirkungen des Verordnungsvorschlags gestaltet sich schwierig, weil an zahlreichen Stellen Ermächtigungen der Kommission zu delegierten Rechtsakten nach Art. 86 bzw. zu Durchführungsrechtsakten nach dem in Art. 87 vorgegebenen Verfahren in dem Vorschlag enthalten sind. Während Durchführungsrechtsakte in einzelnen Bereichen aufgrund erforderlicher Anpassungen an technische Entwicklungen gerechtfertigt sein mögen, erscheinen die umfangreichen Gestaltungsbefugnisse der Kommission in der Gesamtschau als zu weitgehend, da sie eine erhebliche Rechtsunsicherheit für die datenverarbeitende Wirtschaft bedeuten. Nach Art. 290 AEUV kann der Kommission die Befugnis übertragen werden, Rechtsakte ohne Gesetzescharakter mit allgemeiner Geltung zur Ergänzung oder Änderung bestimmter nicht wesentlicher Vorschriften des betreffenden Gesetzgebungsaktes zu erlassen. Es kann nicht angenommen werden, dass die Vielzahl der Vorschriften, die geändert werden können, nicht wesentlich sind. Außerdem müssen bereits die Regelungen der zukünftigen Verordnung hinreichend bestimmt sein. Gerade angesichts der massiven Sanktionsvorschriften muss für die Verantwortlichen von vornherein klar erkennbar sein, wie weit ihre Pflichten gehen.

Position der deutschen Versicherungswirtschaft:

Anstelle von delegierten Rechtsakten sollte das Datenschutzrecht in den einzelnen Sektoren durch Selbstregulierungsmaßnahmen konkretisiert werden. **Die deutsche Versicherungswirtschaft geht diesen Weg gemeinsam mit den deutschen Datenschutzbehörden bereits nach dem aktuellen deutschen Datenschutzrecht (siehe oben Vorbemerkung).** Der Verordnungsvorschlag wählt hierzu in Art. 38 einen richtigen Ansatz. Jedoch sollten die Anforderungen an den Inhalt weniger starr festgelegt werden, um eine breite Akzeptanz und Praktikabilität zu sichern.

Berlin, den 30.03.2012

Stellungnahme

zum Vorschlag der EU-Datenschutzverordnung

KOM(2012) 11/4

vom 25. Januar 2012

Zusammenfassung

Die Deutsche Versicherungswirtschaft unterstützt die Ziele, das Datenschutzrecht in Europa zu vereinheitlichen, die grenzüberschreitende Tätigkeit zu erleichtern und Hemmnisse für den internationalen Datentransfer zu beseitigen.

Angesichts des ohnehin schon hohen Datenschutzstandards z. B. in Deutschland sollte eine Regelung der Rechte der Betroffenen und der Anforderungen an Datenschutz und Datensicherheit jedoch mit Augenmaß erfolgen und unnötige bürokratische Belastungen vermeiden. Regelungen, die erkennbar von Vorfällen in der Internetwirtschaft angestoßen sind und nur für den Bereich des Internets Sinn ergeben, sollten dabei nicht generell und allgemeingültig gemacht werden.

Im Hinblick auf versicherungsspezifische Geschäftsabläufe enthält der Vorschlag der Datenschutz-Grundverordnung noch erhebliche rechtliche Unsicherheiten sowie Bestimmungen, die die Bereitstellung von Versicherungsschutz erheblich erschweren, verteuern und in Teilen sogar gefährden würden.

Die zukünftige Verordnung sollte insbesondere folgende Punkte berücksichtigen:

- Es bedarf einer eindeutigen **Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten** in der Lebens-, Kranken-, Unfall- und Haftpflichtversicherung und Rückversicherung. Sie muss auch inzwischen gebräuchliche und sinnvolle **Datenverarbeitungen im Konzern und unter Beteiligung spezialisierter Dienstleister** erfassen (dazu Ziffer 1).

Gesamtverband der Deutschen
Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5290
Fax: +49 30 2020-6290

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +32 2 28247-39

Ansprechpartner:
Dr. Martina Vomhof
Leiterin
Datenschutz/Grundsatzfragen

E-Mail: m.vomhof@gdv.de

www.gdv.de

- Tarifierung und Risikodifferenzierung als Kernbestandteile des Versicherungsgeschäfts müssen möglich bleiben. Die auf das Internet zugeschnittenen Bestimmungen zur **Profilbildung** (Art. 20) dürfen die Tarifeinstufung und Risikoeinschätzung in der Versicherungswirtschaft nicht erfassen. Die **Begriffsbestimmungen** müssen dahingehend überarbeitet werden, dass die Nutzung weniger sensibler Sachdaten und pseudonymisierter Daten möglich bleibt (dazu Ziffer 2).
- Verfahren zum **Schutz vor Versicherungsbetrug und unzuverlässigen Versicherungsvermittlern** müssen durchführbar bleiben (dazu Ziffer 3).
- Umfangreiche **Betroffenenrechte**, wie das Recht auf Vergessen (Art. 17) und Datenübertragbarkeit (Art. 18), die primär auf soziale Netzwerke im Internet zugeschnitten sind, dürfen die Vertragsdurchführung nicht gefährden (dazu Ziffer 4).
- Die **Anforderungen an Maßnahmen zu Datenschutz und Sicherheit** müssen praktikabel bleiben (dazu Ziffer 5). Die erheblich belastende Datenschutz-Folgenabschätzung (Art. 33) sollte entfallen und die Verpflichtung zur Meldung von Datenpannen auf gravierende Fälle eingeschränkt werden (Art. 31, 32).
- Möglichkeiten zur **kollektiven Rechtsdurchsetzung** sind nicht erforderlich, zumal den Datenschutzaufsichtsbehörden weitgehende Kompetenzen eingeräumt sind (dazu Ziffer 7). **Sanktionen** sollten auf ein verträgliches Maß begrenzt werden (dazu Ziffer 8).
- Die weiten Befugnisse der Europäischen Kommission zum **Erlass von delegierten Rechtsakten** bedeuten Rechtsunsicherheit. Vorzugswürdig ist eine Konkretisierung der Verordnung durch branchenspezifische **Selbstregulierungsmaßnahmen** (dazu Ziffer 9).

Inhaltsübersicht

Vorbemerkung

Als Risikoträger für Unternehmen und private Haushalte erfüllt die Versicherungswirtschaft im Rahmen der gesamten Volkswirtschaft eine essentielle Funktion. Ebenso wie individuelle Eigenvorsorge oder eine staatliche Absicherung zählt die Möglichkeit, sich über einen privaten Versicherungsschutz gegen elementare Lebensrisiken abzusichern, in der sozialen Marktwirtschaft zu den Eckpfeilern der Daseinsvorsorge. Indem die Versicherungswirtschaft private oder öffentliche Risiken übernimmt, schafft sie für Unternehmen und Wirtschaft die Sicherheiten, die notwendig sind, damit sich Initiative und innovatives Unternehmertum überhaupt erst entfalten können. Die Absicherung gegen private Lebensrisiken ermöglicht den Bürgerinnen und Bürgern ein Leben in Freiheit und Sicherheit.

Allein in Deutschland bieten Versicherungsunternehmen mit ca. 450 Millionen Versicherungsverträgen umfassenden Risikoschutz und soziale Sicherheit.

Die deutschen Versicherer sind sich ihrer Verantwortung bewusst, die damit einhergeht, dass sie zur Erfüllung ihrer Aufgaben personenbezogene Daten ihrer Kunden und Antragsteller verarbeiten müssen. Aus diesem Grund erarbeitet der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) zurzeit gemeinsam mit den deutschen Datenschutzbehörden aktuell Verhaltensregeln zum Umgang mit personenbezogenen Daten (Code of Conduct). In engem Zusammenhang mit dieser geplanten Selbstregulierungsmaßnahme steht eine gemeinsam erarbeitete datenschutzrechtliche Einwilligungsklausel für die Lebens- und Krankenversicherung, die seit Januar 2012 von den deutschen Datenschutzbehörden empfohlen wird und auch die nach deutschem Strafrecht geforderte Schweigepflichtentbindung umfasst. Auch der Verbraucherzentrale Bundesverband (vzbv) als wichtigste Interessenvertretung der Verbraucher in Deutschland ist an der Ausarbeitung des Code of Conduct und der Einwilligung beteiligt. Die Versicherungswirtschaft wird damit in Deutschland als erste Branche ein Datenschutzkonzept haben, das von Datenschutzbehörden, Verbraucherschützern und Wirtschaft gemeinsam getragen wird.

Vor diesem Hintergrund begrüßt die deutsche Versicherungswirtschaft das Bestreben der Europäischen Kommission, das Datenschutzrecht in Europa zu vereinheitlichen. Für europaweit tätige Unternehmen bedeutet es eine erhebliche Erleichterung, wenn sie sich nicht mit unterschiedlichen materiellen Datenschutzvorschriften auseinandersetzen müssen.
Anreize zur Implementierung von Codes of Conduct (Art. 38) und Binding Corporate Rules (Art. 43) sind sinnvoll. Jedoch sollten die Anforderungen an den Inhalt nicht zu starr festgelegt werden, um eine breite Akzeptanz und Praktikabilität zu sichern.

Aus Sicht der Versicherungswirtschaft sollte die zukünftige Verordnung insbesondere folgende Punkte berücksichtigen:

1. Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft

a) Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten

Es bedarf einer eindeutigen Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten in der Lebens-, Kranken-, Unfall-, Haftpflicht- und Rückversicherung.

Hintergrund:

In der Kranken-, Lebens- und Unfallversicherung werden Gesundheitsdaten zwingend benötigt, um im Einklang mit versicherungsaufsichtsrechtlichen Bestimmungen die zu versichernden Risiken zu prüfen und um Versicherungsfälle abwickeln zu können.

Beispiele:

- Es kann nur festgestellt werden, ob ein Versicherter Anspruch auf eine Berufsunfähigkeitsrente hat, wenn geprüft worden ist, ob er eine Erkrankung hat, aufgrund derer er seinen Beruf nicht mehr ausüben kann.
- Ein Krankenrücktransport aus dem Ausland kann nur organisiert werden, wenn dem Versicherer oder Assisteur, der den Transport organisiert, bekannt ist, welche Erkrankung der Versicherte hat.
- Rückversicherer, die Risiken von den Erstversicherern ganz oder teilweise übernehmen und damit die Erfüllung der Verträge sicherstellen, benötigen Gesundheitsdaten, um zu prüfen, ob sie das Risiko zeichnen können bzw. im Versicherungsfall dafür einstehen müssen.
- Haftpflichtversicherer können Personenschäden nur abwickeln, wenn sie die Gesundheitsdaten der Geschädigten verarbeiten können.

Ziel muss es sein, die für die soziale Absicherung der Bevölkerung notwendige Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft auf eine rechtssichere Grundlage zu stellen. Sie muss den Interessen der Versicherten und Antragsteller Rechnung tragen, zu denen auch effiziente Prozessabläufe im Rahmen von Risikoprüfung und Schadenabwicklung zählen.

Verordnungsvorschlag der Kommission:

Der Vorschlag enthält **keine ausreichende gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft**. Eine solche gesetzliche Grundlage ist für die Versicherungsbranche – auch nach Überzeugung der deutschen Datenschutzbehörden – dringend erforderlich.

Der Vorschlag enthält zwar viele Ansatzpunkte, die eine **gesetzliche Grundlage** für die notwendige Verarbeitung von Gesundheitsdaten bieten könnten. Jedoch reichen sie nicht aus:

- Art. 9 Abs. 2f) regelt die Verarbeitung zur Begründung, Geltendmachung oder Abwehr von Rechtsansprüchen, nicht aber (wie Art. 6 Abs. 1b) zur Begründung und Durchführung von Verträgen.
- Art. 9 Abs. 2g) dürfte vermutlich nicht angewendet werden, wenn Art. 9 Abs. 2h) i. V. m. Art. 81 der Verordnung als spezielle Erlaubnisnormen für die Verarbeitung von Gesundheitsdaten verstanden werden.
- Nach Art. 9 Abs. 2h) ist die Verarbeitung von Gesundheitsdaten zulässig, wenn sie vorbehaltlich der Bedingungen und Garantien des Art. 81 für „*Gesundheitszwecke***"** erforderlich ist. Damit ist allenfalls die Krankenversicherung erfasst. Inwiefern dies der Fall ist, ist angesichts der Formulierung des Art. 81 Abs. 1c zudem unsicher.

Die Nutzung von **Einwilligungen** als Rechtsgrundlage kann nur eine Notlösung sein. Sie wird den tatsächlichen Geschäftsabläufen nicht gerecht und führt im Ergebnis zu einer Verschlechterung der Situation der Versicherungsnehmer.

Der Vorschlag geht davon aus, dass die betroffene Person eine völlige Entscheidungsfreiheit hat und ihre **Einwilligung jederzeit widerrufen** kann (Art. 7 Abs. 3 und Erwägungsgrund 32). Wenn die Daten zur Durchführung eines Vertrages verarbeitet werden müssen, kann der Kunde theoretisch zwar auf den Vertragsschluss verzichten. Eine Vertragsdurchführung ohne Verarbeitung der Daten ist aber nicht möglich. Bei der inzwischen üblichen Datenverarbeitung in vorgegebenen automatisierten Prozessen, die der Abwicklung von Millionen von Verträgen dient, ist es auch nicht realistisch, dass einzelne Betroffene die Art und Weise der Verarbeitung beeinflussen können.

Die Zulässigkeit der Einwilligungen in der Versicherungswirtschaft wird zudem durch **Art. 7 Abs. 4** des Verordnungsvorschlags infrage gestellt. Danach ist die **Einwilligung** als Rechtsgrundlage der Datenverarbeitung **ausgeschlossen**, wenn zwischen dem Betroffenen und der verantwortlichen Stelle ein **erhebliches Ungleichgewicht** besteht. Nach Erwägungsgrund 34 ist dies der Fall, wenn ein Abhängigkeitsverhältnis besteht, z. B. in Beschäftigungsverhältnissen. Nach der Einschätzung von Datenschutzbehörden ist es auszuschließen, dass ein solches Ungleichgewicht nicht nur zwischen Arbeitgebern und Arbeitnehmern, sondern auch zwischen Versicherungsunternehmen und ihren Kunden oder Geschädigten angenommen wird. Damit wäre eine Einwilligung ausgeschlossen. Ein genereller Ausschluss der Einwilligung in Art. 7 Abs. 4 schränkt Verbraucher in ihrer Entscheidungsfreiheit ein und steht dem eigentlichen Ziel des Datenschutzes entgegen, den Einzelnen als Herrn über seine Daten zu stärken. Die Versicherungswirtschaft stellt er vor große Schwierigkeiten, ihre Datenverarbeitung zu rechtfertigen.

Position der deutschen Versicherungswirtschaft:

Notwendig ist eine eindeutige, europaweit geltende gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten in allen betroffenen Versicherungssparten, also in der Lebens-, Kranken-, Unfall- und Haftpflichtversicherung sowie bei Rückversicherungen. Eine solche gesetzliche Grundlage muss sich auch auf die unternehmensübergreifende Datenverarbeitung im Konzern sowie die Einschaltung von dritten Personen, wie z. B. ärztlichen Gutachtern und Assistance-Unternehmen, erstrecken (dazu unten 2).

Art. 7 Abs. 4 muss unbedingt gestrichen werden.

b) Verarbeitung von Gesundheitsdaten im Konzern und Beteiligung von Dienstleistern

Es bedarf einer Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten im Konzern und die Beteiligung von Dienstleistern.

Hintergrund:

Um Synergien zu erzielen und dem Gebot der Wirtschaftlichkeit zu entsprechen, müssen innerhalb von Versicherungsgruppen ebenso wie in anderen Branchen Serviceaufgaben delegiert und zentralisiert oder an kompetente Dienstleister ausgelagert werden.

Beispiele:

- Die Entgegennahme von Schadensmeldungen, die Überwachung der Schadensabwicklung sowie die Steuerung von Gutachtenaufträgen wird von einem bestimmten Konzernunternehmen oder einem spezialisierten Dienstleister übernommen.
- Ein Unternehmen überträgt die gesamte Risikoprüfung und Schadensbearbeitung für alle Konzerngesellschaften Mitarbeitern der Konzernmutter.
- Erkrankungen werden z. B. in kleineren Gesellschaften immer und bei großen Unternehmen in bestimmten Fällen durch externe Ärzte begutachtet.
- Eine Krankenversorgung im Ausland und Krankenrücktransporte werden durch hierauf spezialisierte Assistance-Gesellschaften durchgeführt.
- Die Versorgung mit medizinischen Hilfsmitteln erfolgt durch Fachbetriebe.

Sowohl diese Maßnahmen als auch die Risikoverlagerung auf Rückversicherer sind nach der Richtlinie 2009/138/EG des Europäischen Parlamentes und des Rates vom 25. November 2009 (betreffend die Aufnahme und Ausübung der Versicherungs- und Rückversicherungstätigkeit – Solvency II) versicherungsaufsichtsrechtlich zulässig.

Vorschlag der Kommission:

Art. 4 Abs. 5 und Art. 24 sind für die Regelung der gemeinsamen Datenverarbeitung nicht hilfreich, weil sie keine eindeutige Ermächtigungsgrundlage für eine Datenweitergabe von einer verantwortlichen Stelle an die andere schaffen. Sobald eine gesamte Aufgabe übertragen wird, liegt nach Auffassung vieler Datenschutzbehörden keine Auftragsdatenverarbeitung vor, sodass Art. 26 nicht eingreift.

Wenn Gesundheitsdaten verarbeitet werden, bedarf es somit grundsätzlich für jede Datenübermittlung einer **Einwilligung** des Betroffenen. Abgesehen von den erheblichen rechtlichen Unsicherheiten einer solchen Einwilligung (dazu oben 1a) und dem damit verbundenen Zeit- und Kostenaufwand erweist sich dieser Weg für alle Veränderungen während der Laufzeit eines Versicherungsvertrages als äußerst unpraktikabel. Nach Abschluss des Vertrages reagiert die Mehrzahl der Betroffenen auf die Bitte zur Abgabe der Erklärung erfahrungsgemäß schlichtweg nicht. Es ist nicht möglich, angesichts notwendiger Veränderungen der Geschäftsprozesse immer wieder jeden einzelnen Versicherungsnehmer erneut um seine Einwilligung zu bitten.

Die Probleme können in der Versicherungswirtschaft nicht einfach gelöst werden, indem Unternehmen zusammengelegt und damit zu einer einheitlichen verantwortlichen Stelle gemacht werden. Denn Versicherungsunternehmen sind gemäß Art. 73 der Richtlinie 2009/138/EG grundsätzlich zur **Spartentrennung** zwischen Lebens- und Nichtlebensversicherung verpflichtet. Diese Versicherungssparten dürfen nur durch verschiedene juristische Personen betrieben werden. In Deutschland gilt das Spartentrennungsgebot zudem für die substitutive Krankenversicherung und für die Leistungsbearbeitung in der Rechtsschutzversicherung. Diese Regeln dienen nur der Trennung der Haftungsmassen, haben aber keinen datenschutzrechtlichen Grund.

Position der deutschen Versicherungswirtschaft:

Anstelle einer Einwilligung, die von vielen Betroffenen ohne Reflektion abgegeben wird und daher oft keinen besonderen Schutz bietet, sollten gesetzliche Anforderungen an die Zulässigkeit der Datenübermittlung zwischen Unternehmen einer Versicherungsgruppe, an Rückversicherungsunternehmen und an Dienstleister geschaffen werden. Wenn sichergestellt ist, dass die Daten nur dem ursprünglichen Zweck entsprechend verarbeitet werden, dass die anderen Unternehmen unter Berücksichtigung der Eignung der von ihnen zu Datenschutz und Datensicherheit getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt sind und dazu vertraglich vereinbart wurde, dass der Geheimnis- und Datenschutz bei dem anderen Unternehmen gewährleistet ist, muss auch eine Übermittlung von Gesundheitsdaten zulässig sein.

Mit dieser gesetzlichen Lösung würden alle Betroffenen geschützt, unabhängig davon, ob sie eine Einwilligung erteilen oder nicht.

c) Verarbeitung von genetischen und biometrischen Daten in der Versicherungswirtschaft

aa) Genetische Daten

Die im Versicherungsgeschäft notwendige Verarbeitung von genetischen Daten muss auf sicherer Rechtsgrundlage möglich sein.

Hintergrund:

Die deutschen Versicherer verlangen weder vor noch nach Abschluss eines Versicherungsvertrages die Durchführung genetischer Untersuchungen. Auf die Ergebnisse vorhandener genetischer Untersuchungen wird im Rahmen des gesetzlich Zulässigen nur bei Abschluss von Verträgen mit sehr hohen Beitragssummen zurückgegriffen. Möglich bleiben muss jedoch die Anzeige bekannter Vorerkrankungen nach Maßgabe des jeweils geltenden Versicherungsvertragsrechts.

Im Rahmen ärztlicher Diagnosen spielt heute neben konventionellen Untersuchungsmethoden häufig die Auswertung genetischer Daten eine Rolle. Welche Art von Krebserkrankung besteht und wie sie behandelt werden kann, kann z. B. konventionell, aber auch anhand genetischer Untersuchungen festgelegt werden. Die Versicherungswirtschaft benötigt Untersuchungsergebnisse für die Risikoprüfung und Leistungsbearbeitung in der Personenversicherung. Die Nutzung der Daten für die Prüfung einer bestehenden, diagnostizierten Erkrankung darf nicht davon abhängen, welche Untersuchungsmethode ein Arzt zugrunde legt.

Verordnungsvorschlag der Kommission:

Nach Art. 4 Abs. 10 sind „genetische Daten“ Daten jedweder Art zu den ererbten oder während der vorgeburtlichen Entwicklung erworbenen Merkmalen eines Menschen. Dieser Begriff der genetischen Daten ist zu weit. Er erfasst z. B. auch das für jedermann sichtbare Geschlecht. Außerdem werden Behinderungen erfasst, die nicht genetisch bedingt sind, sondern während der Schwangerschaft der Mutter, z. B. durch Sauerstoffmangel, erworben wurden.

Art. 9 Abs. 1 bezieht auch „genetische Daten“ in die besonderen Kategorien personenbezogener Daten ein, ohne jedoch hinreichende Ausnahmen festzulegen.

Position der deutschen Versicherungswirtschaft:

Der Begriff der „genetischen Daten“ in Art. 4 Abs. 10 sollte auf mit Untersuchung der DNA, RNA oder der Chromosomen gewonnenen Daten über genetische Eigenschaften eines Menschen begrenzt werden.

Die Nutzung genetischer Daten für die Prüfung einer bestehenden, diagnostizierten Erkrankung muss aber ebenso möglich sein wie die Nutzung der Ergebnisse konventioneller Untersuchungsmethoden, da nicht beeinflussbar ist, welchen Methoden ein Arzt zugrunde legt. Insofern sollten genetische Daten wie Gesundheitsdaten behandelt werden.

bb) Biometrische Rechnungsgrundlagen

Der Begriff der biometrischen Daten muss klar auf „biometrische Erkennungsdaten“ begrenzt werden.

In der Versicherungsmedizin spielen sogenannte „biometrische Rechnungsgrundlagen“ eine Rolle, d. h. physische oder physiologische Merkmale werden in die versicherungsmathematischen Berechnungen einbezogen. Dies dürfte in Art. 4 Abs. 11 hier nicht gemeint sein. Es könnte jedoch zu Verwechslungen mit den gemeinten biometrische Erkennungsdaten kommen.

2. Tarifeinstufung und die Risikoeinschätzung in der Versicherungswirtschaft

a) Abgrenzung von der Profilbildung

Tarifierung und Risikoeinschätzung in der Versicherungswirtschaft müssen klar vom Begriff der Profilbildung in Art. 20 ausgenommen werden.

Hintergrund:

Es entspricht der Natur von Versicherungsverträgen, dass nach bestimmten Kriterien Risikogemeinschaften gebildet werden müssen. Dies geschieht in der Regel aufgrund der statistischen Auswertung bekannter Schadensfälle. Diese werden nach gemeinsamen Merkmalen zusammengefasst und lassen so den statistisch wahrscheinlichen Schadenverlauf der Merkmalsgruppe erkennen. Ein Beispiel dafür sind die in der Versicherungswirtschaft verwendeten Sterbetafeln. Die Wahrscheinlichkeit des Eintritts eines Versicherungsfalls und dessen Ausmaß werden im Einzelfall durch eine Risikoprüfung auf Grundlage der Angaben des Versicherungsnehmers mithilfe der Unternehmensstatistiken sowie weiterer bekannter Wahrscheinlichkeiten, wie medizinischer Erfahrungswerte, bewer-

tet. Der Preis für den Versicherungsschutz wird dann entsprechend der Einordnung festgelegt.

Beispiele:

- In der Elementarschadenversicherung können Häuser, die in einem in regelmäßigen Abständen von Überschwemmungen betroffenen Ort liegen, nicht zu gleichen Konditionen versichert werden wie Häuser, die in einem Ort fernab von Gewässern liegen.
- Ebenso unterscheidet sich die Bemessung eines Beitrags danach, ob ein zu versicherndes Haus ein leicht brennbares Reetdach oder ein feuerfestes Schindeldach hat.
- Ein Hobbypilot kann nicht zu gleichen Bedingungen versichert werden, wie jemand, der kein gefährliches Hobby hat.
- Ein Mensch, der ein schweres Rückenleiden hat, kann in der Berufsunfähigkeitsversicherung nur zu ungünstigeren Bedingungen versichert werden, weil mit höherer Wahrscheinlichkeit Kosten auf die Versichertengemeinschaft zukommen.

Die Datenverarbeitung in der Versicherungswirtschaft wird ausführlich in der Empfehlung des Ministerkomitees des Europarates Rec (2002) 9 an die Mitgliedstaaten über den Schutz von zu Versicherungszwecken erhobenen und verarbeiteten personenbezogenen Daten geregelt. Hier werden auch „aktuarische Aktivitäten“ und damit auch die für die Versicherungswirtschaft wesensnotwendige Tarifierung erlaubt (Empfehlungen 4.4. k). Das Gleiche gilt für die Vorbereitung und den Abschluss der Versicherung, also Tarifeinstufung und Prämienbemessung (Empfehlungen 4.4. a).

Eine ordnungsgemäße Geschäftsorganisation eines Versicherers setzt nach Art. 44 der Solvency II-Rahmenrichtlinie (RL 2009/138/EG) ein angemessenes Risikomanagement voraus. Hierzu gehören auch die Risikoprüfung und -erkennung. Das Gesamtrisiko des Unternehmens ist aus der Aggregation der Einzelrisiken zu ermitteln. Im Rahmen der erforderlichen Risikosteuerung ist die Tarifierung und Risikoeinschätzung zwingend erforderlich.

Die Tarifeinstufung erfolgt in Massensparten teilweise auch automatisiert. Dieser Trend wird sich in der Zukunft fortsetzen.

<u>Verordnungsvorschlag der Kommission:</u>

Der Vorschlag verbietet in Art. 20 grundsätzlich Profilbildungen aufgrund automatisierter Prozesse. Damit soll in erster Linie die Bildung von Verhaltensprofilen aufgrund von Aktivitäten im Internet verhindert werden. Die Bestimmung würde nach ihrem Wortlaut jedoch auch automatisierte Tarifeinstufungen und Risikoeinschätzungen in der Versicherungswirtschaft erfassen und damit die Arbeit der Versicherungswirtschaft im Kern gefährden. Tatsächlich handelt es sich jedoch um grundlegend andere

Sachverhalte. Bei den versicherungstypischen Verfahrensweisen geht es gerade nicht darum, persönliche Präferenzen, Verhaltensweisen oder Einstellungen Einzelner zu analysieren oder vorherzusagen, sondern Gruppen mit gleichartigem Risikobild aufzustellen, um einem einzelnen Versicherten der Gruppe, den zufällig der Versicherungsfall trifft, aus der Summe der Beiträge Ersatz leisten zu können.

Eine **automatisierte Einschätzung aufgrund von Gesundheitsdaten**, z. B. in einer schnell abzuschließenden Reisekrankenversicherung, wäre nach **Art. 20 Abs. 3** generell verboten, selbst wenn das Ergebnis für die Kunden nur positiv ist. Eine solche Konsequenz ist vermutlich nicht gewollt und liegt nicht im Interesse der Kunden, denen die Kostenersparnis und der schnellere Policierungsprozess zugutekommen.

Die Regelung widerspricht auch Art. 9 Abs.1 der E-Commerce-Richtlinie vom 08.06.2000 (RL 2000/31/EG), in der es heißt:

> „Die Mitgliedstaaten stellen sicher, dass ihr Rechtssystem den Abschluss von Verträgen auf elektronischem Wege ermöglicht. Die Mitgliedstaaten stellen insbesondere sicher, dass ihre für den Vertragsabschluss geltenden Rechtsvorschriften weder Hindernisse für die Verwendung elektronischer Verträge bilden noch dazu führen, dass diese Verträge aufgrund des Umstandes, dass sie auf elektronischem Wege zustande gekommen sind, keine rechtliche Wirksamkeit oder Gültigkeit haben."

Die zukünftige Verordnung selbst stellt in diesem Punkt ein „Hindernis für die Verwendung elektronischer Verträge" dar, die durch die E-Commerce-Richtlinie gerade gefördert werden soll.

Position der deutschen Versicherungswirtschaft:

Tarifierung und Risikoeinschätzung in der Versicherungswirtschaft müssen ausdrücklich vom Begriff der Profilbildung in Art. 20 ausgenommen werden.

b) Zu weite Definition der Personenbeziehbarkeit von Daten

Die zu weite Definition personenbezogener Daten führt zu unverhältnismäßigen Einschränkungen bei der Verarbeitung wenig sensibler Sachdaten und pseudonymisierter Daten.

Hintergrund:

Zur Risikoeinschätzung nutzt die Versicherungswirtschaft auch wenig sensible Daten, die zunächst keiner Person zugeordnet sind.

Beispiel:

> In der Naturgefahrenversicherung ziehen Versicherer die frei zugänglichen Gefahrenkarten der öffentlichen Hand heran. So stellen etwa die deutschen Wasserwirtschaftsämter Informationen zu Überschwemmungsgebieten zur Verfügung, der Deutsche Wetterdienst hält Informationen zu Starkregen und Sturm vor. Hinzu kommen auflösungsbeschränkte Luftbilder des Bundesamtes für Kartografie und Geodäsie. Diese Daten sind zunächst nicht auf eine konkrete Person bezogen und von denjenigen, die sie weiterleiten, zumeist auch nicht auf eine bestimmte Person beziehbar.

Verordnungsvorschlag der Kommission:

Der Vorschlag geht in **Art. 4 Abs. 1 und 2** von einem **sehr weiten Begriff der Personenbeziehbarkeit** von Daten aus. Es genügt, dass irgendein Dritter – und nicht nur der für die Verarbeitung Verantwortliche – den Personenbezug herstellen könnte. Zum Begriff der personenbezogenen Daten wird damit die weiteste in der Literatur vertretende Rechtsmeinung zugrunde gelegt. Nicht einmal die Einschränkungen, die die Artikel 29-Datenschutzgruppe in ihrem Working Paper 136 (Stellungnahme 4/2007) zum Begriff „personenbezogene Daten“ vom 20. Juni 2007 gemacht hat, werden berücksichtigt.

Nach der weiten Definition läge in dem Beispielsfall bereits von Anfang an ein personenbeziehbares, also dem personenbezogenen gleichgestelltes Datum vor, weil die Möglichkeit besteht, dass jemand feststellt, dass ein Haus in einem Gebiet liegt, in dem Überschwemmungen häufig sind, und ein anderer dieses Haus einem Eigentümer zuordnen kann. Außerdem gelten für objektive, wenig sensible Sachdaten die gleichen Anforderungen wie für direkte Aussagen zu einer Person.

Da es nach der ausdrücklichen Regelung des Art. 4 Absatz 1 ausreicht, dass irgendjemand die Daten zu einer Kennnummer zuordnen kann, ist mit der Begriffsbestimmung außerdem auch jede Pseudonymisierung von Daten datenschutzrechtlich irrelevant.

Position der deutschen Versicherungswirtschaft:

Um ein **Ausufern des Begriffs der personenbezogenen Daten** und damit eine Verwässerung des Datenschutzrechts zu **vermeiden**, ist es erforderlich, die **Definition einzuschränken**. Es müssen **Privilegierungen für nicht unmittelbar personenbeziehbare Sachdaten sowie pseudonymisierte Daten** geschaffen werden.

Einschränkungen nur für vollständig anonymisierte Daten reichen nicht aus. Sofern für bestimmte Fälle diese Regelung zum Schutz des informationellen Selbstbestimmungsrechts nicht ausreicht, können diese gesondert geregelt werden.

3. Verhinderung von Versicherungsbetrug und Gewährleistung der Zuverlässigkeit von Versicherungsvermittlern

Den Auskunftssystemen der Versicherungswirtschaft zum Schutz vor Versicherungsbetrug und unzuverlässigen Versicherungsvermittlern darf die Rechtsgrundlage nicht entzogen werden.

Hintergrund:

Der deutschen Versicherungswirtschaft entstehen allein in der Schaden- und Unfallversicherung durch Versicherungsbetrug Verluste in einer geschätzten Höhe von vier Milliarden Euro pro Jahr.

> Eine Studie der Gesellschaft für Konsumforschung (GfK) aus dem Jahr 2011 ergab, dass ca. vier Prozent der befragten Haushalte offen zugaben, in den letzten fünf Jahren Versicherungsbetrug begangen zu haben. Weitere ca. sieben Prozent wissen von einem konkreten Versicherungsbetrug. Sonderuntersuchungen haben gezeigt, dass bis zu 40 % der Schäden an Smartphones, Flat-TV's und Laptops in Betrugsabsicht eingereicht wurden.

Diese Kosten verteuern den Versicherungsschutz für redliche Versicherungskunden erheblich. Die Versicherungswirtschaft ist daher im Interesse der Versicherten auf Maßnahmen der Betrugsbekämpfung angewiesen. Dem dient z. B. in Deutschland das **Hinweis- und Informationssystem (HIS)**, das erst im Jahr 2011 nach den Vorgaben der deutschen Datenschutzbehörden neu organisiert wurde. In diesem System werden bestimmte, auf ein erhöhtes Risiko hindeutende Daten aus den Versicherungsunternehmen gespeichert. Darüber hinaus kann es in klar definierten Fällen zu einem Datenaustausch zwischen betroffenen Versicherungsunternehmen kommen.

Auch die **Auskunftsstelle über den Versicherungs- und Bausparaußendienst (AVAD)** verarbeitet Informationen über Vermittler, um im Interesse der Verbraucher deren Zuverlässigkeit sicherzustellen. Satzungsmäßiger Zweck der AVAD ist es, zu erreichen, dass nur vertrauenswürdige Personen Versicherungs-, Bauspar- und sonstige Finanzdienstleistungsprodukte vermitteln. Ihre Tätigkeit dient der Umsetzung der Versicherungsvermittlerrichtlinie (Richtlinie 2002/92/EG des Europäischen Parlaments und des Rates vom 9. Dezember 2002 über Versicherungsvermittlung) in Deutschland. Die Identifizierung und Benennung unlauterer Vermittler ist notwendig, da keine laufende Kontrolle der Vermittler gewährleistet ist. Insbesondere für den Bereich der gebundenen Vermittler findet die Zuverlässigkeitsüberprüfung allein durch die Unternehmen statt. Hier ist die AVAD als Branchenauskunftei ein unverzichtbares Mittel der Überprüfung. Die AVAD ist daher sowohl von der Bundesanstalt für Fi-

nanzdienstleistungsaufsicht, also der deutschen Versicherungsaufsichtsbehörde als auch von den deutschen Datenschutzbehörden anerkannt.

In dem Betrugsbekämpfungssystem HIS werden auch **Verurteilungen wegen Versicherungsbetrugs** gespeichert und können von anderen Versicherern abgefragt werden. Die AVAD speichert ebenfalls **Strafurteile**, die sich auf die Zuverlässigkeit von Versicherungsvermittlern beziehen.

Verordnungsvorschlag der Kommission:

Für den Betrieb von Auskunfteien gibt es in dem Vorschlag für die EU-Datenschutzgrundverordnung **keine klare gesetzliche Grundlage**. Ob Art. 6 Abs. 1f. auch diese Fälle erfassen soll, ist unsicher, weil die Norm hinter Art. 7f) der RL 95/46/EG, der auch eine **Datenverarbeitung im Interesse Dritter** erfasst, zurückbleibt. Damit steht das Hinweis- und Informationssystem (HIS) der deutschen Versicherungswirtschaft, das der Bekämpfung von Versicherungsbetrug dient und auf Wunsch der Datenschutzbehörden gerade erst als Auskunftei ausgestaltet wurde, auf keiner sicheren Rechtsgrundlage mehr. Auch Datenübermittlungen an das System sowie an andere Unternehmen, die heute nach klar umschriebenen Kriterien erlaubt sind, werden zweifelhaft, weil Art. 6 Abs. 1f. des Verordnungsvorschlags keine Datenübermittlung im Interesse Dritter zulässt. Entsprechendes gilt für die Auskunftsstelle über den Versicherungs- und Bausparaußendienst (AVAD).

Durch Art. 9 Abs. 1, 2 (j) wird die Verarbeitung von Daten über Strafurteile an eine rechtlich gerade in diesem Fall sehr unsichere Einwilligung oder ein spezielles nationales oder europäisches Gesetz geknüpft. Ein solches Gesetz liegt zumindest in Deutschland nicht vor.

Position der deutschen Versicherungswirtschaft:

Der Betrieb der genannten Systeme muss sichergestellt werden, indem eine Datenverarbeitung im Interesse Dritter zugelassen wird sowie eine Verarbeitung von Daten über Strafurteile bei erheblichem berechtigtem Interesse unmittelbar aufgrund der Verordnung ermöglicht wird.

4. Betroffenenrechte

Umfangreiche Betroffenenrechte dürfen die Vertragsdurchführung und die Durchführung sinnvoller Geschäftsprozesse nicht gefährden.

Ein effektiver Datenschutz setzt voraus, dass die Betroffenen über die Verarbeitung ihrer Daten informiert sind. Jedoch gehen die Rechte, die den Betroffenen durch die Verordnung eingeräumt werden, weit über das aktuelle Datenschutzniveau aller Mitgliedstaaten hinaus. Sie übersteigen

sogar den als besonders hoch geltenden deutschen Datenschutzstandard. Für die Unternehmen bedeuten umfangreiche Benachrichtigungs- und Auskunftspflichten sowie die Rechte auf Vergessenwerden und auf Datenübertragbarkeit nicht nur erheblichen Bürokratieaufwand. Es besteht auch die Gefahr, dass notwendige und sinnvolle Geschäftsabläufe, die auch im Interesse der Kunden liegen, behindert oder sogar unmöglich gemacht werden. Es muss dabei darauf geachtet werden, dass Regelungen, die für soziale Online-Netzwerke passend sind, nicht 1:1 auf den Offline-Betrieb übertragen werden.

a) Recht auf Vergessenwerden und Löschung

In Art. 17 wird ein umfangreiches **Recht auf Vergessenwerden und Löschung** geregelt.

Art. 17 sieht in Absatz 1 zahlreiche Gründe vor, die zur Löschung der Daten führen müssen, u. a. auch den Widerruf einer Einwilligung (Art. 17 Abs. 1b) bzw. d). Da die Alternativen des Art. 17 Abs. 1 nebeneinanderstehen, gilt dies selbst während eines laufenden Vertrages. Jedoch darf es z. B. nicht möglich sein, dass ein Kunde dem Versicherer den Datenbestand ganz oder zum Teil entzieht und damit eine sachliche Leistungsprüfung unmöglich macht oder sich vorzeitig vom Vertrag löst.

Position der deutschen Versicherungswirtschaft:

Das Recht auf Vergessenwerden muss ausgeschlossen sein, wenn die Daten zur Durchführung eines Vertrages erforderlich sind.

b) Sperrung statt Löschung

Die heutigen technischen Systeme ermöglichen in aller Regel keine vollständige Löschung der Daten. So lassen sich etwa aus auf Speicherplatten fotografisch gesicherten Daten keine Teildateien entfernen. Derartige Speichermethoden werden z. B. in Bereichen verwendet, in denen eingescannte Daten nach Vernichtung der Dokumente unveränderbar zur Verfügung stehen müssen. Die Verpflichtung zur vollständigen Löschung wird damit unerfüllbar. Es kann lediglich der Zugriff unmöglich gemacht werden.

Position der deutschen Versicherungswirtschaft:

Für diesen Fall, dass eine Löschung aus technischen Gründen nicht möglich ist, muss eine Sperrung der Daten ausreichen, wie es z. B. in Deutschland in § 35 Abs. 3 Nr. 3 BDSG vorgesehen ist.

c) Recht auf Datenübertragbarkeit

Ein Recht auf Datenübertragbarkeit nach Art. 18 kann wohl dann sinnvoll angewendet werden, wenn eine Person **eigene Inhalte** in das **Internet** stellt, wie z. B. Fotos oder Texte in sozialen Online-Netzwerken. Es ist auch dann nachvollziehbar, wenn Personen eigene Dateien einem Cloud-Anbieter zur Speicherung überlassen. Bei diesen Internet-Anwendungen muss es grundsätzlich möglich sein, die Inhalte wieder zu entfernen oder einem anderen Anbieter zu übertragen. Jedoch geht der Anwendungsbereich des Art. 18 weit über diese Fallgruppen hinaus.

In der Versicherungswirtschaft werden die Daten gesichert zu Zwecken der Vertragsdurchführung oder Abwicklung von Ansprüchen verarbeitet. Da jedoch auch **strukturierte Formate** verwendet werden, müssten Versicherungsunternehmen nach **Art. 18 Abs. 1** Kopien der von ihnen verarbeiteten Daten in einem für die jeweilige Person weiterverwendbaren strukturierten elektronischen Format zur Verfügung stellen. Da die Datenverarbeitungssysteme für völlig andere Abläufe programmiert sind, wäre das nur mit erheblichem technischen und finanziellen Aufwand möglich und ginge über den Unternehmenszweck weit hinaus.

Noch weiter geht **Art. 18 Abs. 2**, der immer eingreift, wenn eine Person ihre Daten zur Verfügung gestellt hat und die Verarbeitung auf einer Einwilligung oder einem Vertrag basiert. Damit fielen z. B. die meisten Kundendaten darunter, die Versicherer verarbeiten. Eine **Überführung der Daten in andere Systeme** ist nicht nur technisch aufwendig. Sie würde auch für den Kunden keinen Nutzen generieren, da beim neuen Versicherer andere Tarife gelten. Zudem wären aus den Datensätzen Tarifstrukturen und damit Geschäftsgeheimnisse erkennbar, sodass auch erhebliche wettbewerbsrechtliche Bedenken bestehen.

<u>Position der deutschen Versicherungswirtschaft:</u>

In der Versicherungswirtschaft, die die Daten zur Durchführung von Verträgen oder zur Erfüllung von Ansprüchen gesichert verarbeitet, ergibt das Recht auf Datenübertragbarkeit keinen Sinn.

d) Informations- und Auskunftsrechte

Transparenz ist ein wichtiges Element des Datenschutzes. Die Betroffenen sollten daher wissen, wer ihre Daten verarbeitet und im Detail Auskunft erhalten können. Zu umfangreich und praktisch kaum erfüllbar sind die **Informationspflichten** aus Art. 14 und die **Auskunftspflichten** aus Art. 15. Die Informationspflichten nach Art. 14 haben bereits eine Detailtiefe, die für viele Kunden nicht von Interesse sein dürfte. Sie können durch delegierte Rechtsakte noch weiter ausgestaltet werden. Damit gehen sie selbst über das scharfe deutsche Recht deutlich hinaus. Auskunftsrechte

können in Branchen, die wie die Versicherungswirtschaft umfangreiche Daten verarbeiten, uferlos werden, wenn sie nicht spezifiziert werden. Sie müssen dort an ihrer Grenzen stoßen, wo Tatsachen geheimhaltungsbedürftig sind.

Position der deutschen Versicherungswirtschaft:

Den Betroffenen sollten mit Art. 14 nicht umfangreiche Informationen aufgedrängt werden, sondern sie sollten die Informationen erhalten, die sie benötigen, um ihr Auskunftsrecht wahrzunehmen. Auskunftswünsche sollten vom Betroffenen spezifiziert werden, um zielgerichtet antworten zu können und unnötigen Rechercheaufwand zu vermeiden.

Ein Vorbild können die Regelungen im deutschen Recht, §§ 33 und 34 BDSG einschließlich der dort genannten Ausnahmen sein.

5. Vermeidung bürokratischer Belastungen

Im Hinblick auf den ohnehin schon hohen Datenschutzstandard sollte die Regelung der Anforderungen an Datenschutz und Datensicherheit mit Augenmaß erfolgen und unnötige bürokratische Belastungen vermeiden.

Entgegen dem erklärten Ziel der Kommission, Bürokratie abzubauen, bringt die Verordnung erhebliche neue bürokratische Belastungen mit sich. Durch den gesamten Verordnungsvorschlag ziehen sich Anforderungen an die Unternehmen, die ganz erheblichen Verwaltungsaufwand zur Folge haben. Nur bespielhaft genannt seien die detaillierten und umfangreichen Vorschriften zur Erstellung und zum Nachweis von Datenschutzstrategien (Art. 22), zur Implementierung und zum Einsatz datenschutzfreundlicher Technik (Art. 23), zur Dokumentation der Verarbeitungsvorgänge (Art. 28), zur Gewährleistung der Datensicherheit (Art. 30) und zur Zusammenarbeit mit der Aufsichtsbehörde (Art. 29, 34). Diese ohnehin schon umfangreichen Pflichten können in aller Regel von der Kommission noch durch delegierte Rechtsakte weiter konkretisiert oder durch Durchführungsbestimmungen formalisiert werden.

Nachfolgend wird nur auf die besonders einschneidenden Pflichten eingegangen.

a) Datenschutzfolgenabschätzung nach Art. 33

Angesichts der Vielzahl von Verpflichtungen, die bereits bestehen, ist das zusätzliche Erfordernis einer Datenschutzfolgenabschätzung nach Art. 33 nicht nachvollziehbar.

Bereits der **Anwendungsbereich der Norm ist nicht eindeutig**. So stellt sich die Frage, wann ein Verarbeitungsvorgang „konkrete Risiken für die Rechte und Freiheiten betroffener Personen“ birgt. Das Regelbeispiel des Art. 33 Abs. 2a) dürfte so zu verstehen sein, dass zahlreiche Datenverarbeitungen in der Versicherungswirtschaft, wie z. B. die Einstufung in einen Tarif, eine Datenschutzfolgenabschätzung erfordern. Nach Art. 33 Abs. 2 b) scheint die gesamte Datenverarbeitung in der Personenversicherung der Datenschutzfolgenabschätzung zu bedürfen, wenn Gesundheitsdaten von Einzelpersonen erfasst sind. Da die Aufsichtsbehörde für weitere Verarbeitungsvorgänge eine Folgenabschätzung verlangen kann (Art. 33 Abs. 2e), Art. 34 Abs. 2b)), ist der Anwendungsbereich der Regelung unabsehbar. Auch ist nicht klar, welchen **Inhalt und Umfang** die Folgenabschätzung haben soll. Die nähere Bestimmung ist nach Art. 33 Abs. 6 der Kommission überlassen.

Besonders belastend ist die Regelung des **Art. 33 Abs. 4**. Danach muss die **Einschätzung der Betroffenen oder ihrer Repräsentanten** eingeholt werden. Dies führt nicht nur zu erheblichem Bürokratieaufwand, sondern **gefährdet Geschäftsgeheimnisse**. Schließlich ist anzunehmen, dass auf diesem Weg auch der Marktgegenseite geplante Verfahren bekannt werden. Art. 33 in der vorgeschlagenen Fassung stellt damit einen unverhältnismäßigen Eingriff in die unternehmerische Freiheit dar.

Position der deutschen Versicherungswirtschaft:

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.

b) Reaktion auf Datenpannen (Art. 31 und 32)

Die Verpflichtung zur **Meldung von Datenpannen** wird sogar im Vergleich zu dem sehr weitgehenden deutschen Recht sehr strikt ausgestaltet. Nach Art. 4 Abs. 9, 31, 32 genügt bereits jede Zerstörung, jeder Verlust, jede Veränderung oder jeder unberechtigte Zugriff auf personenbezogene Daten. Es kommt weder darauf an, ob die Daten ihrer Art nach besonders schutzwürdig sind noch auf die Schwere und Tragweite des Vorfalls für die Betroffenen. Ein so **weit gefasster Anwendungsbereich** lässt eine **Meldeflut** bei den Aufsichtsbehörden und eine Abstumpfung der immer wieder auch in nichtigen Fällen benachrichtigten Betroffenen befürchten.

Position der deutschen Versicherungswirtschaft:

Art. 31 und 32 sollten 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.

6. One-stop shop

Künftig ist nach Art. 51 Abs. 2 die Aufsichtsbehörde am Hauptsitz eines Unternehmens auch für dessen Zweigniederlassungen zuständig. Für europaweit tätige Unternehmen bedeutet es eine erhebliche Erleichterung, dass Meldungen, Genehmigungs- und Dokumentationserfordernisse nur noch einmal zentral bei der zuständigen Datenschutzbehörde erfolgen müssen.

Allerdings ist dieser Vorteil nur begrenzt, weil die meisten Konzerne so organisiert sind, dass sie rechtlich selbständige Tochtergesellschaften haben. Jede Tochtergesellschaft ist grundsätzlich eine eigene verantwortliche Stelle im Sinne der Verordnung. Für sie ist daher jeweils die Aufsichtsbehörde in dem Mitgliedstaat zuständig, in dem die Tochtergesellschaft ihren Sitz hat. Ob Art. 24 so weit ausgelegt werden kann, dass eine Zuständigkeit nur der Aufsichtsbehörde der Muttergesellschaft begründet werden kann, ist zweifelhaft.

Meldepflichten, Genehmigungs-/ Dokumentationserfordernisse etc. fallen also jeweils pro Tochtergesellschaft und damit mehrfach an. Binding Corporate Rules nach Art. 43 des Verordnungsvorschlags müssen nicht nur von der Konzernmutter zur Genehmigung bei der zuständigen Aufsichtsbehörde eingereicht werden, sondern auch von Tochtergesellschaften in anderen EU-Mitgliedstaaten bei den für sie zuständigen Behörden. Damit bleibt es bei erheblichem Bürokratieaufwand.

7. Kollektive Rechtsdurchsetzung

Über Art. 76 Abs. 1 i. V. m. Art. 75 werden Datenschutzverbände auch zu **Sammelklagen** berechtigt. Es ist jedoch kein Rechtsdurchsetzungsdefizit erkennbar, das derartige Klagen rechtfertigt. Das gilt im Datenschutzrecht noch mehr als im Verbraucherschutzrecht. Zur Ahndung möglicher Daten-

schutzverstöße gibt es hier nämlich – anders als z. B. bei der Überprüfung von AGB – spezielle Datenschutzaufsichtsbehörden, die nach der Verordnung umfangreiche Eingriffsbefugnisse haben. Jeder Betroffene kann sich form- und kostenlos an die Behörden wenden. Nach dem Verordnungsvorschlag soll den Datenschutzbehörden in Art. 76 Abs. 2 sogar eine Klagebefugnis verliehen werden.

8. Sanktionen

Gerade angesichts der oben geschilderten umfangreichen Anforderungen und der hohen Rechtsunsicherheiten escheinen die umfangreichen Sanktionen in Art. 79 sehr einschneidend. Hier sollten aber zunächst die Vorschriften angepasst werden, deren Verletzung sanktioniert wird. Auch für große Unternehmen sollte die Möglichkeit der Verwarnung bei ersten unbeabsichtigten Verstößen (Art. 79 Abs. 3) eröffnet werden.

9. Delegierte Rechtsakte und Durchführungsakte

Eine abschließende Einschätzung der Auswirkungen des Verordnungsvorschlags gestaltet sich schwierig, weil an zahlreichen Stellen Ermächtigungen der Kommission zu delegierten Rechtsakten nach Art. 86 bzw. zu Durchführungsrechtsakten nach dem in Art. 87 vorgegebenen Verfahren in dem Vorschlag enthalten sind. Während Durchführungsrechtsakte in einzelnen Bereichen aufgrund erforderlicher Anpassungen an technische Entwicklungen gerechtfertigt sein mögen, erscheinen die umfangreichen Gestaltungsbefugnisse der Kommission in der Gesamtschau als zu weitgehend, da sie eine erhebliche Rechtsunsicherheit für die datenverarbeitende Wirtschaft bedeuten. Nach Art. 290 AEUV kann der Kommission die Befugnis übertragen werden, Rechtsakte ohne Gesetzescharakter mit allgemeiner Geltung zur Ergänzung oder Änderung bestimmter nicht wesentlicher Vorschriften des betreffenden Gesetzgebungsaktes zu erlassen. Es kann nicht angenommen werden, dass die Vielzahl der Vorschriften, die geändert werden können, nicht wesentlich sind. Außerdem müssen bereits die Regelungen der zukünftigen Verordnung hinreichend bestimmt sein. Gerade angesichts der massiven Sanktionsvorschriften muss für die Verantwortlichen von vornherein klar erkennbar sein, wie weit ihre Pflichten gehen.

<u>Position der deutschen Versicherungswirtschaft:</u>

Anstelle von delegierten Rechtsakten sollte das Datenschutzrecht in den einzelnen Sektoren durch Selbstregulierungsmaßnahmen konkretisiert werden. **Die deutsche Versicherungswirtschaft geht diesen Weg gemeinsam mit den deutschen Datenschutzbehörden bereits nach dem aktuellen deutschen Datenschutzrecht (siehe oben Vorbemerkung).**

Der Verordnungsvorschlag wählt hierzu in Art. 38 einen richtigen Ansatz. Jedoch sollten die Anforderungen an den Inhalt weniger starr festgelegt werden, um eine breite Akzeptanz und Praktikabilität zu sichern.

Berlin, den 30.03.2012

ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN

Artikel 40 ***Allgemeine Grundsätze der Datenübermittlung***	EG 78, 79.
Jedwede Übermittlung von personenbezogenen Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung in ein Drittland oder an eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weitergabe personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation.	
Artikel 41 ***Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses***	EG 80 - 82.
1. Eine Datenübermittlung darf vorgenommen werden, wenn die Kommission festgestellt hat, dass das betreffende Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor dieses Drittlands oder die betreffende internationale Organisation einen angemessenen Schutz bietet. Derartige Datenübermittlungen bedürfen keiner weiteren Genehmigung.	Es ist zu begrüßen, dass die Kommission nicht mehr nur ein angemessenes Schutzniveau einzelner Länder, sondern nun auch einzelner Gebiete, Verarbeitungssektoren und internationale Organisationen feststellen kann.
2. Bei der Prüfung der Angemessenheit des gebotenen Schutzes berücksichtigt die Kommission	Der in Absatz 2 genannte Kriterienkatalog zur Beurteilung der Angemessenheit geht über die in der EU-Datenschutzrichtlinie genannten Kriterien weit hinaus. Die Erweiterung der Prüfkriterien könnte die Verfahrensdauer zur Herbeiführung eines Angemessenheitsbeschlusses erheblich verlängern.
a) die Rechtsstaatlichkeit, die geltenden allgemeinen und sektorspezifischen Vorschriften, insbesondere über die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das Strafrecht, die in dem betreffenden Land beziehungsweise der betreffenden internationalen Organisation geltenden Standesregeln und Sicherheitsvorschriften sowie die Existenz wirksamer und durchsetzbarer Rechte einschließlich wirksamer administrativer und gerichtlicher Rechtsbehelfe für betroffene Personen und insbesondere für in der Union ansässige betroffene Personen, deren personenbezogene Daten übermittelt werden;	
b) die Existenz und die Wirksamkeit einer oder mehrerer in dem betreffenden Drittland beziehungsweise in der betreffenden internationalen Organisation tätiger unabhängiger Aufsichtsbehörden, die für die Einhaltung der Datenschutzvorschriften, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit	

mit den Aufsichtsbehörden der Union und der Mitgliedstaaten zuständig sind, und	
c) die von dem betreffenden Drittland beziehungsweise der internationalen Organisation eingegangenen internationalen Verpflichtungen.	
3. Die Kommission kann durch Beschluss feststellen, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation einen angemessenen Schutz im Sinne von Absatz 2 bietet. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.	
4. In jedem Durchführungsrechtsakt werden der geografische und der sektorielle Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b genannte Aufsichtsbehörde angegeben.	
5. Die Kommission kann durch Beschluss feststellen, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation keinen angemessenen Schutz im Sinne von Absatz 2 dieses Artikels bietet; dies gilt insbesondere für Fälle, in denen die in dem betreffenden Drittland beziehungsweise der betreffenden internationalen Organisation geltenden allgemeinen und sektorspezifischen Vorschriften keine wirksamen und durchsetzbaren Rechte einschließlich wirksamer administrativer und gerichtlicher Rechtsbehelfe für in der Union ansässige betroffene Personen und insbesondere für betroffene Personen, deren personenbezogene Daten übermittelt werden, garantieren. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 oder – in Fällen, in denen es äußerst dringlich ist, das Recht natürlicher Personen auf den Schutz ihrer personenbezogenen Daten zu wahren – nach dem in Artikel 87 Absatz 3 genannten Verfahren angenommen.	
6. Wenn die Kommission die in Absatz 5 genannte Feststellung trifft, wird dadurch jedwede Übermittlung personenbezogener Daten an das betreffende Drittland beziehungsweise an ein Gebiet oder einen Verarbeitungssektor in diesem Drittland oder an die betreffende internationale Organisation unbeschadet der Bestimmungen der Artikel 42 bis 44 untersagt. Die Kommission nimmt zu geeigneter Zeit Beratungen mit dem betreffenden Drittland beziehungsweise mit der betreffenden internationalen Organisation auf, um Abhilfe für die Situation, die aus dem gemäß Absatz 5 erlassenen Beschluss entstanden ist, zu schaffen.	Unklar ist, ob bei einem Beschluss nach Absatz 6 die Artikel 42 bis 44 der Verordnung weiterhin anwendbar sind. Siehe auch Anmerkungen zu Artikel 42 Absatz 1.
7. Die Kommission veröffentlicht im *Amtsblatt der Europäischen Union* eine Liste aller Drittländer beziehungsweise Gebiete und Verarbeitungssektoren von Drittländern und aller internationalen Organisationen, bei denen sie durch Beschluss festgestellt hat, dass diese einen beziehungsweise keinen angemessenen Schutz personenbezogener Daten bieten.	Im Sinne verstärkter Transparenz sollte in dieser Verordnung auch festgelegt werden, wie der Markt bereits im Vorfeld der Veröffentlichung im Amtsblatt über den Beschluss zuungunsten eines Drittlandes etc. informiert wird, damit die Marktteilnehmer alternative Möglichkeiten der Datenübermittlungen rechtzeitig vorbereiten und durchführen können. Gerade bei ablehnenden Beschlüssen im Wege des

	abgekürzten Verfahrens nach Artikel 41 Absatz 5 i.V.m. Artikel 87 Absatz 3 fehlt es insbesondere an dieser Transparenz für die betroffenen Marktteilnehmer, da der Beschluss nicht dem Europäischen Parlament vorab vorgelegt werden muss. **GDV-Vorschlag:** **Absatz 7 wird um einen Satz 2 ergänzt:** **„Stellt die Kommission erste tatsächliche Anhaltspunkte fest, dass ein Drittland beziehungsweise ein Gebiet oder ein Verarbeitungssektor eines Drittlands oder eine internationale Organisation keinen angemessenen Schutz im Sinne von Absatz 2 dieses Artikels bieten könnte, teilt sie diese Bedenken in angemessener Form öffentlich mit.**
8. Sämtliche von der Kommission auf der Grundlage von Artikel 25 Absatz 6 oder Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassenen Beschlüsse bleiben so lange in Kraft, bis sie von der Kommission geändert, ersetzt oder aufgehoben werden.	
Artikel 42 ***Datenübermittlung auf der Grundlage geeigneter Garantien***	EG 83, 84.
1. <u>Hat die Kommission keinen Beschluss nach Artikel 41 erlassen</u>, darf ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermitteln, sofern er in einem rechtsverbindlichen Instrument geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat.	Der Wortlaut suggeriert, dass der Anwendungsbereich des Artikel 42 nur eröffnet ist, wenn die Kommission weder festgestellt hat, dass ein entsprechendes Schutzniveau besteht noch, dass es nicht besteht. Daraus würde umgekehrt folgen, dass mit Vorliegen eines negativen oder positiven Kommissionsbeschlusses die Artikel 42 bis 44 nicht anwendbar wären. Diese Sperrwirkung eines Kommissionsbeschlusses kann insbesondere im Hinblick auf die Auffangfunktion der in Artikel 42 Absatz 2 beschriebenen Garantien nicht gewollt sein. Vielmehr sollten die in Absatz 2 genannten Garantien - so wie es bereits in Artikel 26 Absatz 1 der EU-Datenschutzrichtlinie vorgesehen ist - gerade dann zur Anwendung kommen, wenn die Kommission festgestellt hat, dass es kein angemessenes Schutzniveau gibt. **GDV-Vorschlag:** **„<u>Hat die Kommission keinen Beschluss nach Artikel 41 Absatz 1 erlassen</u>, darf ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermitteln, sofern er in einem rechtsverbindlichen Instrument geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat.“**
2. Die in Absatz 1 genannten geeigneten Garantien können insbesondere bestehen in Form	
a) verbindlicher unternehmensinterner Vorschriften nach Artikel 43;	

b) von der Kommission angenommener Standarddatenschutzklauseln, diese Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren erlassen;	
c) von einer Aufsichtsbehörde nach Maßgabe des in Artikel 57 beschriebenen Kohärenzverfahren angenommener Standarddatenschutzklauseln, sofern diesen von der Kommission allgemeine Gültigkeit gemäß Artikel 62 Absatz 1 Buchstabe b zuerkannt wurde, oder	
d) von Vertragsklauseln, die zwischen dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter und dem Empfänger vereinbart und von einer Aufsichtsbehörde gemäß Absatz 4 genehmigt wurden.	
3. Datenübermittlungen, die nach Maßgabe der in Absatz 2 Buchstabe a, b und c genannten unternehmensinternen Vorschriften und Standarddatenschutzklauseln erfolgen, bedürfen keiner weiteren Genehmigung.	
4. Für Datenübermittlungen nach Maßgabe der in Absatz 2 Buchstabe d dieses Artikels genannten Vertragsklauseln holt der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die vorherige Genehmigung der Aufsichtsbehörde gemäß Artikel 34 Absatz 1 Buchstabe a ein. Falls die Datenübermittlung im Zusammenhang mit Verarbeitungstätigkeiten steht, welche Personen in einem oder mehreren anderen Mitgliedstaaten betreffen oder wesentliche Auswirkungen auf den freien Verkehr von personenbezogenen Daten in der Union haben, bringt die Aufsichtsbehörde das in Artikel 57 genannte Kohärenzverfahren zur Anwendung.	
5. Wenn keine geeigneten Garantien für den Schutz personenbezogener Daten in einem rechtsverbindlichen Instrument vorgesehen werden, holt der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die vorherige Genehmigung für die Übermittlung oder Kategorie von Übermittlungen oder für die Aufnahme von entsprechenden Bestimmungen in die Verwaltungsvereinbarungen ein, die die Grundlage für eine solche Übermittlung bilden. Derartige vorherige Genehmigungen der Aufsichtsbehörde müssen im Einklang mit Artikel 34 Absatz 1 Buchstabe a stehen. Falls die Datenübermittlung im Zusammenhang mit Verarbeitungstätigkeiten steht, welche Personen in einem oder mehreren anderen Mitgliedstaaten betreffen oder wesentliche Auswirkungen auf den freien Verkehr von personenbezogenen Daten in der Union haben, bringt die Aufsichtsbehörde das in Artikel 57 genannte Kohärenzverfahren zur Anwendung. Sämtliche von einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilten Genehmigungen bleiben so lange in Kraft, bis sie von dieser Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden.	

Artikel 43 ***Datenübermittlung auf der Grundlage verbindlicher unternehmensinterner Vorschriften***	EG 85.
1. Eine Aufsichtsbehörde kann nach Maßgabe des in Artikel 58 beschriebenen Kohärenzverfahrens verbindliche unternehmensinterne Vorschriften genehmigen, sofern diese	
a) rechtsverbindlich sind, <u>für alle Mitglieder der Unternehmensgruppe</u> des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters sowie deren Beschäftigte gelten und von diesen Mitgliedern angewendet werden;	Die Geltungspflicht für alle Unternehmen einer Unternehmensgruppe, die der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter angehört, ist zu weit gefasst. Sobald ein Unternehmen einer Unternehmensgruppe den unternehmensinternen Vorschriften im Rahmen seiner unternehmerischen Entscheidungsfreiheit nicht beitritt, scheidet Artikel 43 für die übrigen Unternehmen gänzlich aus. Vor dem Hintergrund, dass große Konzerne mehrere hundert Tochtergesellschaften (z.B. Allianz Group) haben, stellt sich die Frage nach der Verhältnismäßigkeit eines solchen „Alles-oder-nichts-Prinzips“. **GDV-Vorschlag:** **„rechtsverbindlich sind, <u>für ~~alle~~ bestimmte Mitglieder</u> der Unternehmensgruppe des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters sowie deren Beschäftigte gelten und von diesen Mitgliedern angewendet werden.“**
b) den betroffenen Personen ausdrücklich durchsetzbare Rechte übertragen;	
c) die in Absatz 2 festgelegten Anforderungen erfüllen.	
2. Alle verbindlichen unternehmensinternen Vorschriften enthalten mindestens folgende Informationen:	
a) Struktur und Kontaktdaten der Unternehmensgruppe und ihrer Mitglieder;	Die Anforderung, alle Kontaktdaten der Unternehmen einer Unternehmensgruppe in unternehmensinterne Vorschriften aufzunehmen, ist nicht im Interesse der Lesbarkeit und Verständlichkeit dieser Vorschriften. Information, wo eine aktualisierte Liste der Unternehmen einschließlich der Kontaktdaten zu finden ist (z.B im Internet) müsste ausreichen. **GDV-Vorschlag:** **„Struktur der Unternehmensgruppe und ihrer Mitglieder und <u>Hinweise auf deren</u> Kontaktdaten;“**
b) die betreffenden Datenübermittlungen oder Datenübermittlungskategorien einschließlich der betreffenden Kategorien personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;	Diese Verordnung sollte Rahmenvorgaben für unternehmensinternen Vorschriften machen. Die in b) genannten Informationen sind zu eng und übersteigen diesen Rahmen. So führt beispielsweise die Festlegung der betreffenden Drittländer ebenso wie der Zweck der Datenübermittlung in den unternehmensinternen Vorschriften zu einer Beschränkung der Flexibilität, da Veränderungen der Geschäftsprozesse/ Geschäftspartner mit einer „Novellierung“ der unternehmensinternen Vorschriften einhergehen müsste.

c)	Interne und externe Rechtsverbindlichkeit der betreffenden unternehmensinternen Vorschriften;	
d)	die allgemeinen Datenschutzgrundsätze, zum Beispiel Zweckbegrenzung, die Datenqualität, die Rechtsgrundlage für die Verarbeitung sowie die Bestimmungen für etwaige Verarbeitungen sensibler personenbezogener Daten, Maßnahmen zur Sicherstellung der Datensicherheit und die Anforderungen für die Datenweitergabe an nicht an diese Vorschriften gebundene Organisationen;	Es sollten nur allgemeine Aussagen zu der Rechtsgrundlage getroffen werden müssen.
e)	die Rechte der betroffenen Personen und die diesen offen stehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, keiner einer Profilerstellung dienenden Maßnahme nach Artikel 20 unterworfen zu werden sowie des in Artikel 75 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde beziehungsweise auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen unternehmensinternen Vorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;	Das Recht, keiner einer Profilerstellung dienenden Maßnahme nach Artikel 20 unterworfen zu werden, ist eine materiell-rechtliche Regelung, die unmittelbar aus dieser Verordnung stammt. Fest steht, dass die unternehmensinternen Vorschriften für die Datenübermittlung in Drittländer etc. ein Schutzniveau bieten soll, das sich an dieser Verordnung orientiert. Allerdings bedeutet dies nicht, dass materiell-rechtliche Vorgaben dieser Verordnung ohne Konkretisierungsmöglichkeit der betroffenen Unternehmen in die unternehmensinternen Vorschriften Eingang finden. Dies entspricht auch nicht dem Grundgedanken der Selbstregulierung.
f)	die von dem in einem Mitgliedstaat niedergelassenen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter übernommene Haftung für etwaige Verstöße von nicht in der Union niedergelassenen Mitgliedern der Unternehmensgruppe gegen die verbindlichen unternehmensinternen Vorschriften; der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter kann teilweise oder vollständig von dieser Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann;	
g)	die Art und Weise, wie die betroffenen Personen gemäß Artikel 11 über die verbindlichen unternehmensinternen Vorschriften und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte informiert werden;	
h)	die Aufgaben des gemäß Artikel 35 benannten Datenschutzbeauftragten einschließlich der Überwachung der Einhaltung der verbindlichen unternehmensinternen Vorschriften in der Unternehmensgruppe sowie die Überwachung der Schulungsmaßnahmen und den Umgang mit Beschwerden;	
i)	die innerhalb der Unternehmensgruppe bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen unternehmensinternen Vorschriften;	
j)	die Verfahren für die Meldung und Erfassung von Änderungen der Unternehmenspolitik und ihre Meldung an die Aufsichtsbehörde;	Die Offenlegung unternehmensinterner Entscheidungen im Hinblick auf die Unternehmenspolitik ist nicht gerechtfertigt, da nicht erkennbar ist, welcher datenschutzrechtliche Mehrwert dadurch bewirkt wird.

	GDV-Vorschlag: **Absatz 2 j) wird gestrichen.**
k) die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Unternehmensgruppe gewährleisten, wie insbesondere die Offenlegung der Ergebnisse der Überprüfungen der unter Buchstabe i dieses Absatzes genannten Maßnahmen gegenüber der Aufsichtsbehörde.	
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für verbindliche unternehmensinterne Vorschriften im Sinne dieses Artikels und insbesondere die Kriterien für deren Genehmigung und für die Anwendung von Absatz 2 Buchstaben b, d, e, und f auf verbindliche unternehmensinterne Vorschriften von Auftragsverarbeitern sowie weitere erforderliche Anforderungen zum Schutz der personenbezogenen Daten der betroffenen Personen festzulegen.	Die Ermächtigung der Kommission zum Erlass delegierter Rechtsakte bringt erhebliche Rechtsunsicherheit für die Unternehmen mit sich. **GDV-Vorschlag:** **Absatz 3 wird gestrichen.**
4. Die Kommission kann das Format und Verfahren für den auf elektronischem Wege erfolgenden Informationsaustausch über verbindliche unternehmensinterne Vorschriften im Sinne dieses Artikels zwischen für die Verarbeitung Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden festlegen. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.	
Artikel 44 ***Ausnahmen***	EG 86 - 89.
1. Falls weder ein Angemessenheitsbeschluss nach Artikel 41 vorliegt noch geeignete Garantien nach Artikel 42 bestehen, ist eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland oder an eine internationale Organisation nur zulässig, wenn	
a) die betroffene Person der vorgeschlagenen Datenübermittlung zugestimmt hat, nachdem sie über die Risiken derartiger ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien durchgeführter Datenübermittlungen informiert wurde,	
b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist,	
c) die Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem für die Verarbeitung Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich ist,	
d) die Übermittlung aus wichtigen Gründen des öffentlichen Interesses notwendig ist,	

e) die Übermittlung zur Begründung, Geltendmachung oder Verteidigung von Rechtsansprüchen erforderlich ist,	
f) die Übermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,	
g) die Übermittlung aus einem Register erfolgt, das gemäß dem Unionsrecht oder dem mitgliedstaatlichen Recht zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die im Unionsrecht oder im mitgliedstaatlichen Recht festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind, oder	
h) die Übermittlung zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter wahrgenommen wird, erforderlich ist und nicht als <u>häufig oder massiv</u> bezeichnet werden kann, und falls der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter alle Umstände beurteilt hat, die bei einer Datenübermittlung oder bei einer Kategorie von Datenübermittlungen eine Rolle spielen, und gegebenenfalls auf der Grundlage dieser Beurteilung geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat.	Die Einführung dieses – im Vergleich zu Artikel 26 der EU-Datenschutzrichtlinie – neuen Übermittlungstatbestandes ist zu begrüßen, da diese zusätzliche Rechtsgrundlage flexibleres Handeln ermöglicht. Unklar für den Rechtsanwender ist jedoch, was mit „häufig“ oder „massiv“ gemeint ist. Sofern darunter regelmäßige Datenübermittlungen von größerem Umfang verstanden werden, ist zu bedenken, dass angesichts der umfangreichen Anforderungen des Absatzes 3 (Kriterien für die Beurteilung) und 6 (Dokumentationspflichten) dieser Übermittlungstatbestand für die Praxis wenig attraktiv erscheint. Auch im Sinne der Rechtsklarheit sollte auf diese Einschränkung verzichtet werden. **GDV-Vorschlag:** „**die Übermittlung zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter wahrgenommen wird, erforderlich ist ~~und nicht als häufig oder massiv bezeichnet werden kann~~, und falls der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter alle Umstände beurteilt hat, die bei einer Datenübermittlung oder bei einer Kategorie von Datenübermittlungen eine Rolle spielen, und gegebenenfalls auf der Grundlage dieser Beurteilung geeignete Garantien zum Schutz personenbezogener Daten vorgesehen hat.“**
2. Datenübermittlungen gemäß Absatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen Daten umfassen. Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Antrag dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.	
3. Bei Datenverarbeitungen gemäß Absatz 1 Buchstabe h berücksichtigt der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter	

insbesondere die Art der Daten, die Zweckbestimmung und die Dauer der geplanten Verarbeitung, die Situation im Herkunftsland in dem betreffenden Drittland und im Endbestimmungsland sowie erforderlichenfalls etwaige vorgesehene geeignete Garantien zum Schutz personenbezogener Daten.	
4. Absatz 1 Buchstaben b, c und h gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.	
5. Das in Absatz 1 Buchstabe d genannte öffentliche Interesse muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt, anerkannt sein.	
6. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die in Absatz 1 Buchstabe h dieses Artikels genannten geeigneten Garantien in der Dokumentation gemäß Artikel 28 und setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis.	Es fehlt an einer Konkretisierung, wie oft und in welchem Umfang die Aufsichtsbehörden von der Übermittlung in Kenntnis gesetzt werden sollen. Diese Konkretisierung sollte in der Verordnung selbst erfolgen. Aufgrund der vorhandenen Kapazitäten bei den Aufsichtsbehörden spricht vieles für eine einmalige Benachrichtigung der Aufsichtsbehörde zu Beginn der Datenübermittlungsprozesse.
7. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die in Absatz 1 Buchstabe d genannten „wichtigen Gründe des öffentlichen Interesses“ zu präzisieren und die Kriterien und Anforderungen für die geeigneten Garantien im Sinne des Absatzes 1 Buchstabe h festzulegen.	Die Ermächtigung der Kommission sollte sich ausschließlich auf die Präzisierung der Kriterien und Anforderungen für die geeigneten Garantien im Sinne des Absatzes 1 Buchstabe h konzentrieren. Die Frage, ob gegebenenfalls Garantien erforderlich sind, obliegt weiterhin dem für die Verarbeitung Verantwortlichen, der dies auf der Grundlage der nach Absatz 1 Buchstabe h vorzunehmenden Beurteilung eigenständig festlegt. **GDV-Vorschlag:** **„Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die in Absatz 1 Buchstabe d genannten „wichtigen Gründe des öffentlichen Interesses“ zu präzisieren und soweit der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter geeignete Garantien im Sinne des Absatzes 1 Buchstabe h bestimmen, diesbezügliche Kriterien und Anforderungen festzulegen.“**
Artikel 45 ***Internationale Zusammenarbeit zum Schutz personenbezogener Daten***	EG 90, 91.
1. In Bezug auf Drittländer und internationale Organisationen treffen die Kommission und die Aufsichtsbehörden geeignete Maßnahmen zur	
a) Entwicklung wirksamer Mechanismen der internationalen Zusammenarbeit, durch die die Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten erleichtert wird,	
b) gegenseitigen Leistung internationaler Amtshilfe bei der Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten, unter anderem durch Mitteilungen, Beschwerdeverweisungen, Amtshilfe bei Untersuchungen und Informationsaustausch, sofern geeignete Garantien für den Schutz personenbezogener Daten und	

anderer Grundrechte und Grundfreiheiten bestehen,	
c) Einbindung maßgeblich Beteiligter in Diskussionen und Tätigkeiten, die zum Ausbau der internationalen Zusammenarbeit bei der Durchsetzung von Rechtsvorschriften über den Schutz personenbezogener Daten dienen,	
d) Förderung des Austauschs und der Dokumentation von Rechtsvorschriften und Praktiken zum Schutz personenbezogener Daten.	
2. Zu den in Absatz 1 genannten Zwecken ergreift die Kommission geeignete Maßnahmen zur Förderung der Beziehungen zu Drittländern und internationalen Organisationen und insbesondere zu deren Aufsichtsbehörden, wenn sie gemäß Artikel 41 Absatz 3 durch Beschluss festgestellt hat, dass diese einen angemessenen Schutz bieten.	

VERHALTENSREGELN UND ZERTIFIZIERUNG

Artikel 38 ***Verhaltensregeln***	EG 76.
1. Die Mitgliedstaaten, die Aufsichtsbehörden und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Datenverarbeitungsbereiche zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen und sich insbesondere auf folgende Aspekte beziehen:	Die in Absatz 1 a) bis h) dargelegten Anforderungen sollten nicht als Mindestinhalt verstanden werden. Artikel 27 der EU-Datenschutzrichtlinie und die Umsetzungsnorm des § 38a BDSG kommen ohne diese Konkretisierung aus. Bislang gab es keine schlechten Erfahrungen, vielmehr ermöglichte die offene Formulierung den erforderlichen Gestaltungsspielraum zur Abdeckung der branchenspezifischen Besonderheiten. Gerade f) und h) betreffen nicht jedes Unternehmen oder jede Unternehmensbranche und sollten daher nicht zwingend bzw. künstlich geregelt werden. Auch wenn die Formulierung „insbesondere“ eine nicht abschließende Aufzählung impliziert, kann nicht ausgeschlossen werden, dass Absatz 1 a) bis h) in der Anwendung als Mindestmaß für Verhaltensregeln verstanden wird. **GDV-Vorschlag:** **„Die Mitgliedstaaten, die Aufsichtsbehörden und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Datenverarbeitungsbereiche zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen und sich insbesondere auf folgende Aspekte beziehen können:“**
a) faire und transparente Datenverarbeitung,	
b) Datenerhebung,	
c) Unterrichtung der Öffentlichkeit und der betroffenen Personen;	
d) von betroffenen Personen in Ausübung ihrer Rechte gestellte Anträge;	
e) Unterrichtung und Schutz von Kindern;	
f) Datenübermittlung in Drittländer oder an internationale Organisationen;	
g) Mechanismen zur Überwachung und zur Sicherstellung der Einhaltung der Verhaltensregeln durch die diesen unterliegenden für die Verarbeitung Verantwortlichen;	
h) außergerichtliche Verfahren und sonstige Streitschlichtungsverfahren zur Beilegung von Streitigkeiten zwischen für die Verarbeitung Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten unbeschadet der den	

betroffenen Personen aus den Artikeln 73 und 75 erwachsenden Rechte.	
	Es sollte nicht in das Ermessen der Aufsichtsbehörden gestellt werden, ob sie zur Frage der Vereinbarkeit Stellung nehmen möchten. Der Verordnungsvorschlag impliziert durch die Wortwahl „kann“ in Satz 2 jedoch gerade einen Entscheidungsspielraum der Behörden, der vor dem Hintergrund der zunehmenden Bedeutung von Verhaltensregeln nicht gerechtfertigt ist. **GDV-Vorschlag:** **Satz 2 wird wie folgt formuliert.** **„Die Aufsichtsbehörde nimmt zu der Frage Stellung, ob der betreffende Entwurf von Verhaltensregeln beziehungsweise der Änderungsvorschlag mit dieser Verordnung vereinbar ist.“**
2. Verbände und andere Einrichtungen, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern in einem Mitgliedstaat vertreten und beabsichtigen, eigene Verhaltensregeln aufzustellen oder bestehende Verhaltensregeln zu ändern oder zu erweitern, können diesbezügliche Vorschläge der Aufsichtsbehörde in dem betreffenden Mitgliedstaat zur Stellungnahme vorlegen. Die Aufsichtsbehörde kann zu der Frage Stellung nehmen, ob der betreffende Entwurf von Verhaltensregeln beziehungsweise der Änderungsvorschlag mit dieser Verordnung vereinbar ist. Die Aufsichtsbehörde hört die betroffenen Personen oder ihre Vertreter zu diesen Vorschlägen an.	Im Übrigen entspricht die Regelung im Wesentlichen Artikel 27 Absatz 2 der EU-Datenschutzrichtlinie bzw. § 38 a Absatz 1 und 2 BDSG, die sich in der Praxis bewährt haben. Es fehlt jedoch an einer Übergangsregelung. Es ist sicherzustellen, dass ein einmal positiv ergangener Bescheid einer Datenschutzaufsichtsbehörde, wie z.B. in Deutschland nach § 38a Absatz 2 BDSG auch nach Anwendungsbeginn dieser Verordnung gem. Artikel 91 Absatz 2 der Verordnung weitergilt, soweit die ihm zugrunde gelegten Verhaltensregeln mit dieser Verordnung vereinbar sind. Der für die Versicherungswirtschaft eingeführte Code of Conduct sieht eine Evaluierungspflicht nach Änderung der Rechtslage vor. Ergibt diese Evaluierung, dass der Code of Conduct der Verordnung entspricht, sollte die Bestandskraft des Bescheides uneingeschränkt gelten. **GDV-Vorschlag:** **Absatz 2 wird um einen Satz 4 und 5 ergänzt:** **„Mit Beginn der Anwendung nach Artikel 91 Absatz 2 dieser Verordnung legen Verbände und andere Einrichtungen den zuständigen Aufsichtsbehörden einen Bericht zur Evaluierung ihrer bestehenden Verhaltensregeln im Hinblick auf die Vereinbarkeit mit dieser Verordnung vor. Soweit die Aufsichtsbehörden auf Grundlage des Evaluierungsberichts von der Vereinbarkeit mit dieser Verordnung ausgehen, gelten die nach bisheriger Rechtslage erteilten verbindlichen Vereinbarkeitserklärungen fort“.**
3. Verbände und andere Einrichtungen, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern in mehreren Mitgliedstaaten vertreten, können der Kommission Entwürfe von Verhaltensregeln sowie Vorschläge zur Änderung oder Ausweitung bestehender Verhaltensregeln	Die Vorschrift bewirkt eine zweifache Prüfung der Verhaltensregeln auf ihre Vereinbarkeit mit der Verordnung. Absatz 2 gilt für die nationalen Aufsichtsbehörden, Absatz 3 für die EU-Kommission. Der Prüfungsgegenstand ist bei beiden Verfahren derselbe, da anders als in Artikel 27 der EU-Datenschutzrichtlinie nicht zwischen

vorlegen.	„einzelstaatlichen“ und „gemeinschaftlichen“ Verhaltensregeln unterschieden wird. **GDV-Vorschlag:** **„Verbände und andere Einrichtungen, die Kategorien von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern in mehreren Mitgliedstaaten vertreten, können der Kommission Entwürfe von gemeinschaftlichen Verhaltensregeln sowie Vorschläge zur Änderung oder Ausweitung bestehender gemeinschaftlicher Verhaltensregeln vorlegen.“**
4. Die Kommission kann im Wege einschlägiger Durchführungsrechtsakte beschließen, dass die ihr gemäß Absatz 3 vorgeschlagenen Verhaltensregeln beziehungsweise Änderungen und Erweiterungen bestehender Verhaltensregeln allgemeine Gültigkeit in der Union besitzen. Die genannten Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.	Die von der EU-Kommission auf ihre Vereinbarkeit mit der Verordnung nach Absatz 3 geprüften Verhaltensregeln können für allgemein gültig erklärt werden. Anders als bisher bewirkt damit nicht mehr der selbstbestimmte Beitritt eines Unternehmens die rechtliche Verbindlichkeit der Verhaltensregeln. Die Selbstverpflichtung erfolgt in diesen Fällen nicht mehr freiwillig. Darüber hinaus bestehen massive Bedenken gegen diese Kompetenz der Kommission, da diese mit weitreichenden Folgen für die Unternehmen bei eingeschränkter Beteiligungs- und Prüfkompetenzen der Mitgliedstaaten einhergeht. **GDV-Vorschlag:** **Absatz 4 wird gestrichen.**
5. Die Kommission trägt dafür Sorge, dass die Verhaltensregeln, denen gemäß Absatz 4 allgemeine Gültigkeit zuerkannt wurde, in geeigneter Weise veröffentlicht werden.	Es wird auf die Ausführungen zu Absatz 4 verwiesen. **GDV-Vorschlag:** **Absatz 5 wird gestrichen.**
Artikel 39 ***Zertifizierung***	EG 77.
1. Die Mitgliedstaaten und die Kommission fördern insbesondere auf europäischer Ebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und –zeichen, anhand deren betroffene Personen rasch das von für die Verarbeitung Verantwortlichen oder von Auftragsverarbeitern gewährleistete Datenschutzniveau in Erfahrung bringen können. Die datenschutzspezifischen Zertifizierungsverfahren dienen der ordnungsgemäßen Anwendung dieser Verordnung und tragen den Besonderheiten der einzelnen Sektoren und Verarbeitungsprozesse Rechnung.	Zertifizierungssysteme sind grundsätzlich zu begrüßen. Aufwand und Kosten einer Zertifizierung sind zu berücksichtigen. Vor diesem Hintergrund sollte an den bereits bestehenden Zertifizierungsverfahren festgehalten werden. Die Zertifizierung Dritter, die für den für die Verarbeitung Verantwortlichen tätig sind und dazu Daten verarbeiten, wäre sehr zu begrüßen. Durch die Zertifizierung von Auftragsdatenverarbeitern (z.B. im Bereich des Cloud Computing) könnten die vertraglichen Pflichten und deren Kontrolle nach Artikel 26 Absatz 2 dieser Verordnung erheblich reduziert werden. Darüber hinaus könnten bestimmte Datenverarbeitungsprozesse des für die Verarbeitung Verantwortlichen zertifiziert werden. Im Gegenzug sollten die Unternehmen von bürokratischen Belastungen wie dem Nachweis einer Datenschutzstrategie (Artikel 22), der Dokumentation (Artikel 28) oder der der Datenschutzfolgenabschätzung (Artikel 33) befreit werden.

2. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren einschließlich der Bedingungen für die Erteilung und den Entzug der Zertifizierung sowie der Anforderungen für die Anerkennung der Zertifizierung in der Union und in Drittländern festzulegen.	Da es sich bei den Kriterien und Anforderungen für die in Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren um eine „wesentliche“ Regelung handelt, sollte diese Verordnungen selbst diesbezügliche Vorgaben machen und entsprechende Kriterien und Anforderungen für das Zertifizierungsverfahren an dieser Stelle regeln. **GDV-Vorschlag:** **Absatz 2 wird gestrichen.**

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 I: Artikel 1 bis 10

Stand: 2. Mai 2012

KAPITEL I
ALLGEMEINE BESTIMMUNGEN

Artikel 1 ***Gegenstand und Ziele***	EG 1- 10.
a) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.	
b) Die Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.	
c) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt oder verboten werden.	
Artikel 2 ***Sachlicher Anwendungsbereich***	EG 11 - 18.
1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.	
2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten, die vorgenommen wird.	
a) im Rahmen einer Tätigkeit, die nicht in den Geltungsbereich des Unionsrechts fällt, etwa im Bereich der nationalen Sicherheit,	
b) durch die Organe, Einrichtungen, Ämter und	

Agenturen der Europäischen Union,	
c) durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Kapitel 2 des Vertrags über die Europäische Union fallen,	
d) durch natürliche Personen zu ausschließlich persönlichen oder familiären Zwecken ohne jede Gewinnerzielungsabsicht,	
e) zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen durch die zuständigen Behörden.	
3) Die vorliegende Verordnung lässt die Anwendung der Richtlinie 2000/31/EG und speziell die Vorschriften der Artikel 12 bis 15 dieser Richtlinie zur Verantwortlichkeit von Anbietern von Vermittlungsdiensten unberührt.	
Artikel 3 ***Räumlicher Anwendungsbereich***	EG 19 - 22.
1) Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt.	
2) Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen, wenn die Datenverarbeitung	
a) dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten, oder	
b) der Beobachtung ihres Verhaltens dient.	
3) Die Verordnung findet Anwendung auf jede Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen an einem Ort, der nach internationalem Recht dem Recht eines Mitgliedstaats unterliegt.	
Artikel 4 ***Begriffsbestimmungen***	
Im Sinne dieser Verordnung bezeichnet der Ausdruck	
(1)„betroffene Person" eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt mit Mitteln bestimmt werden kann, die der für die Verarbeitung Verantwortliche oder jede sonstige natürliche oder juristische Person nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde, etwa mittels Zuordnung zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen,	Zum Begriff der personenbezogenen Daten wird die weiteste in der Literatur vertretende Rechtsmeinung zugrunde gelegt. Nicht einmal die Einschränkungen, die die Artikel 29 Datenschutzgruppe in ihrem Working Paper 136 (Stellungnahme 4/2007) zum Begriff „personenbezogene Daten" vom 20. Juni 2007 gemacht hat, werden berücksichtigt. Da nach der ausdrücklichen Regelung des Artikels 4 Abs. 1 ausreicht, dass irgendjemand die Daten zu einer Kennnummer zuordnen kann, ist mit der Begriffsbestimmung praktisch jede

wirtschaftlichen, kulturellen oder sozialen Identität sind;	Pseudonymisierung von Daten datenschutzrechtlich irrelevant. Bei der weiten Auslegung kann auch das Abstellen auf Standortdaten zu einer ausufernden Anwendung führen. <u>Beispiel</u>: In der Naturgefahrenversicherung ziehen Versicherer die frei zugänglichen Gefahrenkarten der öffentlichen Hand heran. So stellen etwa die deutschen Wasserwirtschaftsämter Informationen zu Überschwemmungsgebieten zur Verfügung, der Deutsche Wetterdienst hält Informationen zu Starkregen und Sturm vor. Hinzu kommen auflösungsbeschränkte Luftbilder des Bundesamtes für Kartografie und Geodäsie. Diese Daten sind zunächst nicht auf eine konkrete Person bezogen und von denjenigen, die sie weiterleiten, zumeist auch nicht auf eine bestimmte Person beziehbar. Nach der weiten Definition läge bereits von Anfang an ein personenbezogenes Datum vor, weil die Möglichkeit besteht, dass jemand feststellt, dass ein Haus in einem Gebiet liegt, in dem Überschwemmungen häufig sind, und dieses Haus einem Eigentümer zuordnen kann. Um das Datenschutzrecht auf seine wesentliche Schutzfunktion zurückführen zu können, ist eine Einschränkung des Begriffs der personenbezogenen Daten erforderlich. Zumindest sollten Privilegierungen für nicht unmittelbar personenbeziehbare Sachdaten sowie pseudonymisierte Daten geschaffen werden. **GDV-Vorschlag:** **Art. 4 Abs.1 wird wie folgt gefasst:** ***„‘betroffene Person‘ eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt mit Mitteln bestimmt werden kann, die der für die Verarbeitung Verantwortliche ~~oder jede sonstige natürliche oder juristische Person~~ nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde, …;“***
(2)„personenbezogene Daten" alle Informationen, die sich auf eine betroffene Person beziehen;	EG 23, 24. Siehe Anmerkung zu Abs. 1.
(3)„Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, der Abgleich oder die Verknüpfung sowie das Löschen oder Vernichten der Daten;	Vgl. EG 13.
(4)„Datei" jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten	

Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;	
(5)"für die Verarbeitung Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke, Bedingungen und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke, Bedingungen und Mittel der Verarbeitung von personenbezogenen Daten durch einzelstaatliches oder Unionsrecht vorgegeben, können der für die Verarbeitung Verantwortliche beziehungsweise die Modalitäten seiner Benennung nach einzelstaatlichem oder Unionsrecht bestimmt werden;	Die Formulierung „allein oder gemeinsam mit anderen“ genügt auch i. V. m. Art. 24 nicht als Ermächtigungsgrundlage für eine insbesondere für die Versicherungswirtschaft dringend erforderliche gemeinsame Datenverarbeitung im Konzern. Der GDV schlägt für den Bereich der Versicherungswirtschaft eine Ergänzung in einem neuen Art. 81a vor, vgl. Punkt 1 b) der Stellungnahme vom 30.03.2012 (S. 9). Siehe auch Anmerkungen zu Art. 24.
(6)"Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;	
(7)"Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, an die personenbezogene Daten weitergegeben werden;	
(8)"Einwilligung der betroffenen Person" jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte explizite Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;	EG 25.
(9)"Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder widerrechtlich, oder zur unbefugten Weitergabe von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;	Die Melde- und Benachrichtigungspflichten in Artikel 31, 32 sind bei einer so weiten Definition der Verletzung des Schutzes personenbezogener Daten unverhältnismäßig und bergen die Gefahr der Abstumpfung der Betroffenen (vgl. auch den eingeschränkten Vorschlag des Consultive Committees zu Artikel 7 der Konvention Nr. 108 des Europarates). Siehe auch Anmerkungen zu Artikel 31, 32.
(10)„genetische Daten“ Daten jedweder Art zu den ererbten oder während der vorgeburtlichen Entwicklung erworbenen Merkmalen eines Menschen;	Der Begriff der genetischen Daten ist sehr weit. Er erfasst auch das für jedermann sichtbare Geschlecht. Außerdem werden Behinderungen erfasst, die nicht genetisch bedingt sind, sondern während der Schwangerschaft der Mutter, z. B. durch Sauerstoffmangel, erworben wurden. Die Definition sollte daher präziser sein. Im Rahmen ärztlicher Diagnosen spielt heute neben konventionellen Untersuchungsmethoden häufig die Auswertung genetischer Daten eine Rolle. Beispiel: Bei einer Störung der Blutgerinnung ist die Bestimmung genetischer Komponenten mittlerweile üblich. Die Verpflichtung zu einer unterschiedlichen Behandlung von Gesundheits- und genetischen Daten würde angesichts heutiger Arztberichte, die

	vielfach beide Datenarten enthalten, die Versicherungswirtschaft vor unlösbare Probleme stellen. Genetische Daten müssen insofern wie Gesundheitsdaten behandelt werden. **GDV-Vorschlag:** **Art. 4 Abs. 10 wird wie folgt gefasst:** ***„Genetische Daten sind die durch eine Untersuchung der DNA, RNA oder der Chromosomen gewonnenen Daten über genetische Eigenschaften eines Menschen. Genetische Daten sind wie Gesundheitsdaten zu behandeln.“***
(11)„biometrische Daten“ Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Menschen, die dessen eindeutige Identifizierung ermöglichen, wie Gesichtsbilder oder daktyloskopische Daten;	In der Versicherungsmedizin spielen sogenannte „biometrische Rechnungsgrundlagen“ eine Rolle, d. h., physische oder physiologische Merkmale werden in die versicherungsmathematischen Berechnungen einbezogen. Dies dürfte hier nicht gemeint sein, sondern „biometrische Erkennungsdaten“. **GDV-Vorschlag:** **In Art. 4 Abs. 11 wird *„biometrische Daten“* durch *„biometrische Erkennungsdaten“* ersetzt.**
(12)„Gesundheitsdaten“ Informationen, die sich auf den körperlichen oder geistigen Gesundheitszustand einer Person oder auf die Erbringung von Gesundheitsleistungen für die betreffende Person beziehen;	EG 26.
(13)„Hauptniederlassung“ im Falle des für die Verarbeitung Verantwortlichen der Ort seiner Niederlassung in der Union, an dem die Grundsatzentscheidungen hinsichtlich der Zwecke, Bedingungen und Mittel der Verarbeitung personenbezogener Daten getroffen werden; wird über die Zwecke, Bedingungen und Mittel der Verarbeitung personenbezogener Daten nicht in der Union entschieden, ist die Hauptniederlassung der Ort, an dem die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen in der Union hauptsächlich stattfinden. Im Falle des Auftragsverarbeiters bezeichnet „Hauptniederlassung“ den Ort, an dem der Auftragsverarbeiter seine Hauptverwaltung in der Union hat;	EG 27.
(14)„Vertreter“ jede in der Union niedergelassene natürliche oder juristische Person, die von dem für die Verarbeitung Verantwortlichen ausdrücklich bestellt wurde und in Bezug auf die diesem nach dieser Verordnung obliegenden Verpflichtungen an seiner Stelle handelt und gegenüber den Aufsichtsbehörden oder sonstigen Stellen in der	

Union als Ansprechpartner fungiert;	
(15)„Unternehmen“ jedes Gebilde, das eine wirtschaftliche Tätigkeit ausübt, unabhängig von seiner Rechtsform, das heißt vor allem natürliche und juristische Personen sowie Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;	
(16)„Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;	EG 28.
(17)„verbindliche unternehmensinterne Datenschutzregelungen“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines EU-Mitgliedstaats niedergelassener für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter für Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe in einem oder mehreren Drittländern verpflichtet;	
(18)„Kind“ jede Person bis zur Vollendung des achtzehnten Lebensjahres;	EG 29. Die Bestimmung anhand des Alters ist klarer als eine Berücksichtigung der individuellen Einsichtsfähigkeit und bringt damit mehr Rechtssicherheit. Einige Regelungen zu Kindern sind allerdings problematisch, vgl. unten.
(19)„Aufsichtsbehörde“ eine von einem Mitgliedstaat nach Maßgabe von Artikel 46 eingerichtete staatliche Stelle.	

KAPITEL II
Grundsätze

Artikel 5 ***Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten***	EG 30.
Personenbezogene Daten müssen	
a) auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;	Die Nachvollziehbarkeit für die jeweils betroffene Person ist eine sehr weitreichende Forderung. Die für die Versicherungswirtschaft notwendige automatisierte Risikoprüfung kann durchaus sehr komplex aufgebaut sein, sodass nicht immer gewährleistet sein kann, dass dies für alle Kunden nachvollziehbar ist. Es kann allenfalls auf eine objektive Nachvollziehbarkeit, z. B. für Wirtschaftsprüfer, abgestellt werden. **GDV-Vorschlag:** **Art. 5 a) wird wie folgt gefasst:** ***„auf rechtmäßige Weise und nach dem Grundsatz von Treu und Glauben verarbeitet werden;“***
b) für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;	
c) dem Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Datenverarbeitung notwendige Mindestmaß beschränkt sein; sie dürfen nur verarbeitet werden, wenn und solange die Zwecke der Verarbeitung nicht durch die Verarbeitung von anderen als personenbezogenen Daten erreicht werden können;	Wünschenswert wäre eine Privilegierung von pseudonymisierten Daten (dazu oben zu Art. 4 (1)),
d) sachlich richtig und auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unzutreffend sind, unverzüglich gelöscht oder berichtigt werden;	
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, jedoch höchstens so lange, wie es für die Realisierung der Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, wenn die Daten ausschließlich zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke im Einklang mit den Vorschriften und Modalitäten des Artikels 83 verarbeitet werden und die Notwendigkeit ihrer weiteren Speicherung in regelmäßigen Abständen überprüft wird;	Artikel 10 sollte wegen des Sachzusammenhangs hier angefügt bzw. es sollte darauf verwiesen werden.
f) unter der Gesamtverantwortung des für die Verarbeitung Verantwortlichen verarbeitet werden, der dafür haftet, dass bei jedem Verarbeitungsvorgang die Vorschriften dieser Verordnung eingehalten werden, und der den	Eine Nachweispflicht, die sich auf jeden konkreten Verarbeitungsvorgang, also die Abbildung jedes Prozessschrittes und Operators, bezieht, bedeutet erheblichen Aufwand und Kosten für die Unternehmen.

Nachweis hierfür erbringen muss.	
Artikel 6 ***Rechtmäßigkeit der Verarbeitung***	EG 31, 35 - 40.
1. Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:	
a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere genau festgelegte Zwecke gegeben.	
b) Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich oder zur Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen.	
c) Die Verarbeitung ist zur Erfüllung einer gesetzlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt.	Hierdurch wird die Datenverarbeitung aufgrund gesetzlicher Erlaubnis, die in § 4 Abs. 1 BDSG enthalten ist, ausgeschlossen. Der Gesetzgeber - zumindest der europäische - sollte allgemein aber weiter in der Lage sein, Datenverarbeitungen in Spezialbereichen zu gestatten. Das Abstellen auf eine gesetzliche Verpflichtung ist zu eng, weil inzwischen auch andere Rechtsvorschriften, wie bspw. „Delegated Acts“ eine wesentliche Rolle für Wirtschaftsunternehmen spielen. Das Gleiche gilt für Normen von Tarifverträgen und Betriebsvereinbarungen. **GDV-Vorschlag:** **Art. 6 Abs. 1 c) wird wie folgt gefasst:** ***„Die Verarbeitung ist zur Erfüllung einer auf Gesetz oder einer anderen Rechtsvorschrift beruhenden Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt.*** ***‚d) Die Verarbeitung ist durch eine Rechtsvorschrift der Europäischen Union erlaubt.“‘***
d) Die Verarbeitung ist nötig, um lebenswichtige Interessen der betroffenen Person zu schützen.	
e) Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt und die dem für die Verarbeitung Verantwortlichen übertragen wurde.	
f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Dieser gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.	Interessen Dritter: Eine Abwägung mit den Interessen Dritter ist anders als bisher in Art. 7 (f) der RL 94/46/EG nicht vorgesehen. Damit wird die Tätigkeit aller Auskunfteien in Frage gestellt. Beispiele: Mangels einer Vorschrift zu Auskunfteien steht das Hinweis- und Informationssystem (HIS) der deutschen

	Versicherungswirtschaft, das der Bekämpfung von Versicherungsbetrug dient (dazu ausführlich Anmerkung zu Art. 9 Abs. 2 j) und auf Wunsch der Datenschutzbehörden gerade erst als Auskunftei ausgestaltet wurde, auf keiner sicheren Rechtsgrundlage mehr. Das Gleiche gilt für die Auskunftstelle über den Versicherungs- und Bausparaußendienst (AVAD). Die AVAD wurde in Deutschland eingerichtet, um im Interesse der Verbraucher die Zuverlässigkeit von Versicherungsvermittlern sicherstellen und ist sowohl von der Bundesanstalt für Finanzdienstleistungsaufsicht als auch von den Datenschutzbehörden anerkannt. Ihre Tätigkeit dient der Umsetzung der Versicherungsvermittlerrichtlinie (Richtlinie 2002/92/EG des Europäischen Parlaments und des Rates vom 9. Dezember 2002 über Versicherungsvermittlung). <u>Kinder:</u> Die Formulierung zu Kindern ist zweideutig. Nach der ungünstigsten Auslegung ist die Legitimation aufgrund einer Interessenabwägung bei Minderjährigen kategorisch ausgeschlossen - dann wäre etwa auch die Einbindung von Dienstleistern bei der Bearbeitung von Versicherungsverträgen von Kindern unmöglich. **GDV-Vorschlag:** **Art. 6 Abs. 1 f) Satz 1 wird wie folgt gefasst:** ***„Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen <u>oder eines Dritten</u> erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. <u>Auf besondere Interessen von Kindern ist zu achten</u>.“***
2. Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu historischen oder statistischen Zwecken oder für wissenschaftliche Forschungszwecke unterliegt den Bedingungen und Garantien des Artikels 83.	
3. Die Verarbeitungen gemäß Absatz 1 Buchstaben c und e müssen eine Rechtsgrundlage haben im	
a) Unionsrecht oder	
b) Recht des Mitgliedstaats, dem der für die Verarbeitung Verantwortliche unterliegt.	
Die einzelstaatliche Regelung muss ein im öffentlichen Interesse liegendes Ziel verfolgen oder zum Schutz der Rechte und Freiheiten Dritter erforderlich sein, den Wesensgehalt des Rechts auf den Schutz personenbezogener Daten wahren und in einem angemessenen Verhältnis zu dem mit der Verarbeitung verfolgten legitimen Zweck stehen.	

4. Ist der Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten erhoben wurden, nicht vereinbar, muss auf die Verarbeitung mindestens einer der in Absatz 1 Buchstaben a bis e genannten Gründe zutreffen. Dies gilt insbesondere bei Änderungen von Geschäfts- und allgemeinen Vertragsbedingungen.	Die Möglichkeit der Zweckänderung ist zu eng. Sie kommt nicht aufgrund einer Interessenabwägung (f) in Betracht. Hiermit bringt die Vorschrift zu wenig Flexibilität! Beispiel: Je nach Auslegung von „Vereinbarkeit“ könnte es künftig ausgeschlossen sein, einem Versicherungskunden mit einer Hausratsversicherung einen Bausparvertrag anzubieten. Hier kann die Information des Betroffenen über die Zweckänderung einen möglichen Ausgleich darstellen. **GDV-Vorschlag:** **Art. 6 Abs. 4 Satz 1 wird wie folgt gefasst:** ***„Ist der Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten erhoben wurden, nicht vereinbar, muss auf die Verarbeitung mindestens einer der in Absatz 1 Buchstaben a bis f genannten Gründe zutreffen.“***
5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Anwendung von Absatz 1 Buchstabe f für verschiedene Bereiche und Verarbeitungssituationen einschließlich Situationen, die die Verarbeitung personenbezogener Daten von Kindern betreffen, näher zu regeln.	
Artikel 7 ***Einwilligung***	EG 32 - 34.
1. Der für die Verarbeitung Verantwortliche trägt die Beweislast dafür, dass die betroffene Person ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten für eindeutig festgelegte Zwecke erteilt hat.	
2. Soll die Einwilligung durch eine schriftliche Erklärung erfolgen, die noch einen anderen Sachverhalt betrifft, muss das Erfordernis der Einwilligung äußerlich erkennbar von dem anderen Sachverhalt getrennt werden.	
3. Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.	Eine Einwilligung muss dann widerruflich sein, wenn tatsächlich eine völlige Freiheit besteht, sie zu erteilen. Das ist nicht der Fall, solange eine Datenerhebung und -verarbeitung, die zur Durchführung eines Vertrages erforderlich ist, auf eine Einwilligung gestützt werden muss. Ein Beispiel hierfür ist die Verarbeitung von Gesundheitsdaten im Rahmen der Durchführung von Versicherungsverträgen (siehe Anmerkungen zu Art. 9 Abs. 2 h und Art. 81). Durch die uneingeschränkte Widerruflichkeit kann die Vertragsabwicklung unmöglich werden. Ein teilweiser Widerruf kann dazu führen, dass die Prüfung des Risikos oder des Versicherungsfalles nicht mehr durchführbar ist. Hierzu hat die deutsche Versicherungswirtschaft mit den Datenschutzbehörden eine interessengerechte

	Lösung gefunden, wonach ein Widerruf nach den Grundsätzen von Treu und Glauben ausgeschlossen sein oder zur Nichterbringung der Leistung führen kann, wenn die Einwilligung zur Durchführung des Vertrags oder zur Schadensabwicklung erforderlich ist. **GDV-Vorschlag:** **In Art. 7 Abs. 3 wird am Ende ein neuer Satz 3 eingefügt:** ***„Ist die Einwilligung zur Durchführung eines Vertrages erforderlich, kann ein Widerruf nach den Grundsätzen von Treu und Glauben ausgeschlossen sein.“***
4. Die Einwilligung bietet keine Rechtsgrundlage für die Verarbeitung, wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht.	In einigen Versicherungssparten werden Gesundheitsdaten zwingend benötigt, um im Einklang mit versicherungsaufsichtsrechtlichen Bestimmungen die Risiken zu prüfen und um Versicherungsfälle abzuwickeln. Da keine ausreichende gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft vorliegt (dazu Anmerkungen zu Art. 9 Abs. 2 h und Art. 81) ist die Versicherungswirtschaft darauf angewiesen, von Kunden und Antragstellern datenschutzrechtliche Einwilligungen einzuholen. Die deutsche Versicherungswirtschaft hat hierzu aktuell eine neue datenschutzrechtliche Mustereinwilligung mit den deutschen Datenschutzbehörden abgestimmt, die die notwendigen Datenverarbeitungsprozesse erfasst. Art. 7 Abs. 4 stellt die Zulässigkeit derartiger Einwilligungen in Frage, da zu befürchten ist, dass ein erhebliches Ungleichgewicht nicht nur in Beschäftigungsverhältnissen und gegenüber Behörden, sondern auch zwischen großen Unternehmen und ihren Kunden angenommen wird. Ein solch genereller Ausschluss der Einwilligung schränkt Verbraucher in ihrer Entscheidungsfreiheit ein und steht dem eigentlichen Ziel des Datenschutzes entgegen, den Einzelnen als Herrn über seine Daten zu stärken. Die Versicherungswirtschaft stellt er vor große Schwierigkeiten, ihre Datenverarbeitung zu rechtfertigen. Art. 7 Abs. 4 muss daher unbedingt gestrichen werden. Kritisch ist die Norm auch im Hinblick auf Beschäftigungsverhältnisse, die nach Erwägungsgrund 34 eindeutig unter den Anwendungsbereich fallen. Art. 7 Abs. 4 würde dazu führen, dass auch freiwillige Angebote eines Arbeitgebers, wie z. B. zusätzliche Direktversicherungen im Rahmen der Betrieblichen Altersversorgung und Unfallversicherungen für Mitarbeiter nicht möglich wären. Das Gleiche gilt z. B. für freiwillige Fortbildungsmaßnahmen oder Personalentwicklungsprogramme. Eine Einwilligung muss hier möglich bleiben.

	GDV-Vorschlag: **Art. 7 Abs. 4 wird gestrichen.**
Artikel 8 ***Verarbeitung personenbezogener Daten eines Kindes***	
1. Für die Zwecke dieser Verordnung ist die Verarbeitung personenbezogener Daten eines Kindes bis zum vollendeten dreizehnten Lebensjahr, dem direkt Dienste der Informationsgesellschaft angeboten werden, nur rechtmäßig, wenn und insoweit die Einwilligung hierzu durch die Eltern oder den Vormund des Kindes oder mit deren Zustimmung erteilt wird. Der für die Verarbeitung Verantwortliche unternimmt unter Berücksichtigung der vorhandenen Technologie angemessene Anstrengungen, um eine nachprüfbare Einwilligung zu erhalten.	
2. Absatz 1 lässt das allgemeine Vertragsrecht der Mitgliedstaaten, etwa die Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags mit einem Kind, unberührt.	
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Modalitäten und Anforderungen in Bezug auf die Art der Erlangung einer nachprüfbaren Einwilligung gemäß Absatz 1 näher zu regeln. Dabei zieht die Kommission spezifische Maßnahmen für Kleinst- und Kleinunternehmen sowie mittlere Unternehmen in Betracht.	
4. Die Kommission kann Standardvorlagen für spezielle Arten der Erlangung einer nachprüfbaren Einwilligung gemäß Absatz 1 festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.	
Artikel 9 ***Verarbeitung besonderer Kategorien von personenbezogenen Daten***	EG 41 - 44.
1. Die Verarbeitung personenbezogener Daten, aus denen die Rasse oder ethnische Herkunft, politische Überzeugungen, die Religions- oder Glaubenszugehörigkeit oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, sowie von genetischen Daten, Daten über die Gesundheit oder das Sexualleben oder Daten über Strafurteile oder damit zusammenhängende Sicherungsmaßregeln ist untersagt.	
2. Absatz 1 gilt nicht in folgenden Fällen:	
a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten vorbehaltlich der in den Artikeln 7 und 8 genannten Bedingungen eingewilligt, es sei denn, nach den Rechtsvorschriften der Union oder eines Mitgliedstaats kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden, oder	

b) die Verarbeitung ist erforderlich, damit der für die Verarbeitung Verantwortliche seine ihm aus dem Arbeitsrecht erwachsenden Rechte ausüben und seinen arbeitsrechtlichen Pflichten nachkommen kann, soweit dies nach den Vorschriften der Union oder dem Recht der Mitgliedstaaten, das angemessene Garantien vorsehen muss, zulässig ist, oder	
c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen oder einer anderen Person erforderlich und die betroffene Person ist aus physischen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben, oder	
d) die Verarbeitung erfolgt auf der Grundlage angemessener Garantien durch eine politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Erwerbszweck im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung nur auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die Daten nicht ohne Einwilligung der betroffenen Personen nach außen weitergegeben werden, oder	
e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder	
f) die Verarbeitung ist zur Begründung, Geltendmachung oder Abwehr von Rechtsansprüchen erforderlich oder	Ob und inwieweit hieraus die Legitimation für die Verarbeitung von Gesundheitsdaten zum Abschluss bzw. zur Durchführung von Versicherungsverträgen entnommen werden kann, ist unsicher, weil die Formulierung des Art. 6 Abs. 1 b gerade nicht übernommen wurde. Zur Notwendigkeit einer Regelung siehe Anm. zu Art. 9 Abs. 2 h).
g) die Verarbeitung ist erforderlich, um auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene Garantien zur Wahrung der berechtigten Interessen der betroffenen Person vorsieht, eine im öffentlichen Interesse liegende Aufgabe zu erfüllen, oder	Ob hieraus die Grundlage für eine EU- oder nationale Regelung für die Verarbeitung von Gesundheitsdaten zum Abschluss von Versicherungsverträgen hergeleitet werden kann ist zweifelhaft, weil Art. 9 Abs. 2 h) als Sonderregelung verstanden werden könnte und weil auch der ähnlich formulierte Art. 8 Abs. 4 der RL 95/46/EG bisher zum Teil nicht als ausreichende Rechtsgrundlage angesehen wurde. Zur Notwendigkeit einer Regelung siehe Anm. zu Art. 9 Abs. 2 h).
h) die Verarbeitung betrifft Gesundheitsdaten und ist vorbehaltlich der Bedingungen und Garantien des Artikels 81 <u>für Gesundheitszwecke</u> erforderlich oder	<u>Zu enge Formulierung:</u> Eine Begrenzung auf die Verarbeitung <u>für Gesundheitszwecke</u> ist zu eng. Sie würde die Fallgruppen des Art. 81 Abs. 1 c) nicht vollständig erfassen. <u>Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten in der Versicherungswirtschaft:</u> In der Krankenversicherung, der Lebensversicherung und der Unfallversicherung werden Gesundheitsdaten

	zwingend benötigt, um im Einklang mit versicherungsaufsichtsrechtlichen Bestimmungen die Risiken prüfen und um Versicherungsfälle abzuwickeln zu können. Auch Rückversicherer, die Risiken ganz oder teilweise übernehmen, benötigen diese Daten. Haftpflichtversicherer brauchen zur Abwicklung von Personenschäden die Gesundheitsdaten der Geschädigten. Die deutsche Versicherungswirtschaft hat hierzu aktuell eine neue datenschutzrechtliche Mustereinwilligung mit den deutschen Datenschutzbehörden abgestimmt, aus der die notwendigen Datenverarbeitungsprozesse hervorgehen. Wie in den Anmerkungen zu Art. 7 dargestellt wurde, ist eine Einwilligung eine äußerst unsichere Grundlage für die Datenverarbeitung. Notwendig ist eine eindeutige, europaweit geltende gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten in den betroffenen Versicherungssparten. Sie könnte in einen neuen Art. 81a der Verordnung aufgenommen werden Formulierungsvorschlag (siehe Stellungnahme des GDV, Ziffer 1 a), S. 5 ff.). Genetische Daten: Im Rahmen ärztlicher Diagnosen spielt heute neben konventionellen Untersuchungsmethoden häufig die Auswertung genetischer Daten eine Rolle. Beispiel: Die Versicherungswirtschaft benötigt diese Daten wie Gesundheitsdaten (dazu Anmerkungen zu Art. 4 (10). **GDV-Vorschlag:** (*kann entfallen, wenn dem Vorschlag zu Art. 4 (10) vollständig gefolgt wird)* **Art. 9 Abs. 2 h) wird wie folgt gefasst:*„h) die Verarbeitung betrifft Gesundheitsdaten oder genetische Daten, soweit diese der Feststellung oder Therapie einer bestehenden Erkrankung dienen,.und ist vorbehaltlich der Bedingungen und Garantien des Art. 81 und Art. 81a ~~für Gesundheitszwecke~~ erforderlich oder“***
i) die Verarbeitung ist vorbehaltlich der Bedingungen und Garantien des Artikels 83 für historische oder statistische Zwecke oder zum Zwecke der wissenschaftlichen Forschung erforderlich oder	
j) die Verarbeitung von Daten über Strafurteile oder damit zusammenhängende Sicherungsmaßregeln erfolgt entweder unter behördlicher Aufsicht oder aufgrund einer gesetzlichen oder rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt, oder zur Erfüllung einer Aufgabe, der ein wichtiges öffentliches Interesse zugrunde liegt, soweit dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das angemessene Garantien vorsehen muss, zulässig ist. Ein vollständiges Strafregister darf nur unter	Der Versicherungswirtschaft entstehen allein in der Schaden- und Unfallversicherung durch Versicherungsbetrug Verluste in einer geschätzten Höhe von 4 Milliarden Euro pro Jahr. Eine Studie der GfK, Gesellschaft für Konsumforschung aus dem Jahr 2011 ergab, dass ca. 4 % der befragten Haushalte offen zugaben, in den letzten 5 Jahren Versicherungsbetrug begangen zu haben. Weitere ca. 7 % wissen von einem konkreten Versicherungsbetrug. Sonderuntersuchungen ergaben, dass bis zu 40 % der Schäden an

behördlicher Aufsicht geführt werden.	Smartphones, Flat-TV's und Laptops in Betrugsabsicht eingereicht wurden. Diese Kosten verteuern den Versicherungsschutz für redliche Versicherungskunden erheblich. Die Versicherungswirtschaft ist im Interesse der Versicherten auf Maßnahmen der Betrugsbekämpfung angewiesen. Dem dient in Deutschland das Hinweis- und Informationssystem (HIS), das erst im Jahr 2011 nach den Vorgaben der Datenschutzbehörden neu organisiert wurde. In dem System werden auch Verurteilungen wegen Versicherungsbetruges gespeichert und können von anderen Versicherern abgefragt werden. Auch die Auskunftsstelle über den Versicherungs- und Bausparaußendienst (AVAD) verarbeitet strafrechtliche Daten, um im Interesse der Verbraucher die Zuverlässigkeit von Vermittlern sicherstellen. Ihre Tätigkeit dient der Umsetzung der Versicherungsvermittlerrichtlinie (Richtlinie 2002/92/EG des Europäischen Parlaments und des Rates vom 9. Dezember 2002 über Versicherungsvermittlung) in Deutschland und ist sowohl von der Bundesanstalt für Finanzdienstleistungsaufsicht als auch von den Datenschutzbehörden anerkannt. Durch Art. 9 Abs. 1, 2 (j) wird die Verarbeitung von Daten über Strafurteile jedoch an eine rechtlich gerade in diesem Fall sehr unsichere Einwilligung oder ein spezielles deutsches oder europäisches Gesetz geknüpft. Ein solches Gesetz liegt zumindest in Deutschland nicht vor. Der Betrieb der genannten Systeme muss sichergestellt werden, entweder durch ein noch zu erlassendes Gesetz oder besser durch die Schaffung einer entsprechenden Ausnahme in der Verordnung selbst. **GDV-Vorschlag:** **Art. 9 Abs. 2 j) wird wie folgt gefasst:** ***„die Verarbeitung von Daten über Strafurteile oder damit zusammenhängende Sicherungsmaßregeln erfolgt entweder unter behördlicher Aufsicht oder aufgrund einer gesetzlichen oder rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt, oder zur Wahrnehmung eines wichtigen öffentlichen Interesses oder sonstigen erheblichen berechtigten Interesses, das die schutzwürdigen Interessen der Betroffenen deutlich überwiegt. ~~zugrunde liegt, soweit dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das angemessene Garantien vorsehen muss, zulässig ist.~~ Ein vollständiges Strafregister darf nur unter behördlicher Aufsicht geführt werden."***
3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Modalitäten sowie angemessene	Die Ausgestaltungsbefugnisse der Kommission führen zu erheblichen Rechtsunsicherheiten, wann die Verarbeitung von besonderen Kategorien

Garantien für die Verarbeitung der in Absatz 1 genannten besonderen Kategorien von personenbezogenen Daten und die in Absatz 2 genannten Ausnahmen näher zu regeln.	personenbezogener Daten zulässig ist. Es handelt sich um sowohl für die Betroffenen wesentliche als auch für die Verarbeiter wirtschaftlich bedeutsame Aspekte, die in der Verordnung eindeutig geregelt werden müssen.
Artikel 10 ***Verarbeitung, ohne dass die betroffene Person bestimmt werden kann***	EG 45.
Kann der für die Verarbeitung Verantwortliche anhand der von ihm verarbeiteten Daten eine natürliche Person nicht bestimmen, ist er nicht verpflichtet, zur bloßen Einhaltung einer Vorschrift dieser Verordnung zusätzliche Daten einzuholen, um die betroffene Person zu bestimmen.	Diese wichtige Regelung sollte in den Sachzusammenhang zu Artikel 5 gezogen werden.

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 11 bis 21

Stand: 20. Juni 2012

KAPITEL III
RECHTE DER BETROFFENEN PERSON

ABSCHNITT 1
TRANSPARENZ UND MODALITÄTEN

Artikel 11 ***Transparente Information und Kommunikation***	EG 46.
1. Der für die Verarbeitung Verantwortliche verfolgt in Bezug auf die Verarbeitung personenbezogener Daten und die Ausübung der den betroffenen Personen zustehenden Rechte eine nachvollziehbare und für jedermann leicht zugängliche Strategie.	Es ist unklar, was genau eine „nachvollziehbare und für jedermann leicht zugängliche Strategie“ darstellt. Sie sollte in Art. 11 Abs. 1 genauer definiert werden. Dies gilt umso mehr, als Art. 79 Abs. 6 e scharfe Sanktionen für das Unterlassen der Festlegung interner Datenschutzstrategien festlegt, von denen man annehmen muss, dass sie auch für Verstöße nach Art. 11 Abs. 1 gelten (Art. 79 Abs. 6 e bedarf diesbezüglich einer Klarstellung.). Eine vollkommene **Offenlegung der Strategie ist zur Vermeidung des Bekanntwerdens von Geschäftsgeheimnissen nicht möglich**. Es wäre denkbar, dass damit die Datenschutz-Politik gemeint ist. Ist dies der Fall, so sollte es in Absatz 1 deutlich gemacht werden. Die Nachvollziehbarkeit kann sich nur auf Fachleute beziehen. **GDV-Vorschlag:** **Art. 11 Abs. 1 wird wie folgt gefasst:** „Der für die Verarbeitung Verantwortliche verfolgt in Bezug auf die Verarbeitung personenbezogener Daten und die Ausübung der den betroffenen Personen zustehenden Rechte eine **für die Datenschutzbehörden nachvollziehbare Datenschutzpolitik**.“
2. Der für die Verarbeitung Verantwortliche stellt der betroffenen Person alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten in	Es ist nicht möglich, die Informationen auf den unterschiedlichen Empfängerhorizont aller Adressaten zuzuschneiden. Dies würde einen zu großen Bürokra-

verständlicher Form unter Verwendung einer klaren, einfachen und adressatengerechten Sprache zur Verfügung, besonders dann, wenn die Information an ein Kind gerichtet ist.	tieaufwand mit sich bringen. Es wäre daher ausreichend, eine ‚klare und einfache Sprache' zu fordern (siehe unten). Dies sollte auch im Hinblick auf die in Art. 79 Abs. 5 a enthaltenen Sanktionen für Auskünfte gelten, welche „nicht oder nicht vollständig oder in nicht hinreichend transparenter Weise" übermittelt werden. (Auch Art. 79 Abs. 5 a bedarf diesbezüglich einer Klarstellung, wann Auskünfte die genannten Anforderungen erfüllen oder nicht.) **GDV-Vorschlag:** **Art. 11 Abs. 2 wird wie folgt gefasst:** „Der für die Verarbeitung Verantwortliche stellt der betroffenen Person alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten in verständlicher Form **unter Verwendung einer klaren und einfachen Sprache** zur Verfügung, besonders dann, wenn die Information an ein Kind gerichtet ist."
Artikel 12 ***Verfahren und Vorkehrungen, damit die betroffene Person ihre Rechte ausüben kann***	EG 47, 48.
1. Der für die Verarbeitung Verantwortliche legt fest, mittels welcher Verfahren er die Informationen gemäß Artikel 14 bereitstellt und den betroffenen Personen die Ausübung der ihnen gemäß Artikel 13 sowie den Artikeln 15 bis 19 zustehenden Rechte ermöglicht. Er trifft insbesondere Vorkehrungen, um die Beantragung der in Artikel 13 sowie in den Artikeln 15 bis 19 genannten Maßnahmen zu erleichtern. Im Falle der automatischen Verarbeitung personenbezogener Daten sorgt der für die Verarbeitung Verantwortliche dafür, dass die Maßnahme elektronisch beantragt werden kann.	
2. Der für die Verarbeitung Verantwortliche kommt seiner Informationspflicht gegenüber der betroffenen Person umgehend nach und teilt ihr spätestens innerhalb eines Monats nach Eingang eines Antrags mit, ob eine Maßnahme nach Artikel 13 oder den Artikeln 15 bis 19 ergriffen wurde, und erteilt die erbetene Auskunft. Diese Frist kann um einen Monat verlängert werden, wenn mehrere betroffene Personen von ihren Rechten Gebrauch machen und ihre Zusammenarbeit bis zu einem vertretbaren Maß notwendig ist, um einen unnötigen und unverhältnismäßig hohen Aufwand seitens des für die Verarbeitung Verantwortlichen zu vermeiden. Die Unterrichtung hat schriftlich zu erfolgen. Stellt die betroffene Person den Antrag in elektronischer Form, ist sie auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.	Frist: Die **Frist** für die Beantwortung eines Antrages sollte **erst dann beginnen, wenn der Antragsteller alle relevanten Informationen zur Bearbeitung seines Antrags zur Verfügung gestellt** hat. Name und Anschrift sind möglicherweise nicht ausreichend, damit ein Versicherer eine Fehlmeldung abgeben kann. Denn der Adressbestand ist möglicherweise nicht auf dem aktuellsten Stand, wenn der Kunde eine Adressänderung nicht mitgeteilt hat. Da hier stets geprüft werden muss, ob die jeweiligen Bestände auch Daten Dritter oder andere nicht zu offenbarende Daten enthalten, ist auch die Monatsfrist bzw. die Verlängerungsmöglichkeit in Satz 2 zu eng. Die Verlängerung um einen weiteren Monat kann zu knapp sein, wenn z. B. massenhaft Auskunftsportale im Internet genutzt werden. **GDV-Vorschlag:** **Art. 12 Abs. 2 Satz 1 und 2 werden wie folgt gefasst:** „Der für die Verarbeitung Verantwortliche kommt seiner Informationspflicht gegenüber der betroffenen Person umgehend nach und teilt ihr spätestens innerhalb eines Monats nach Eingang eines **vollständigen** Antrags **mit allen zur Bearbeitung relevanten In-**

	formationen mit, ob eine Maßnahme nach Artikel 13 oder den Artikeln 15 bis 19 ergriffen wurde, und erteilt die erbetene Auskunft. Diese Frist kann ~~**um einen Monat**~~ verlängert werden, wenn mehrere betroffene Personen von ihren Rechten Gebrauch machen **oder die begehrte Maßnahme einen erhöhten Aufwand erfordert, insbesondere wegen des Umfangs oder der erforderlichen Prüfung der berechtigten Interessen Dritter.**~~**, um einen unnötigen und unverhältnismäßig hohen Aufwand seitens des für die Verarbeitung Verantwortlichen zu vermeiden.**~~" Form: Es ist **nicht ersichtlich, wie die Verpflichtung zur elektronischen Form den Interessen der Betroffenen dienen soll**. Dagegen kann es für Unternehmen eine unnötige und damit bürokratische Belastung darstellen, verschiedene Formen der Unterrichtung bereithalten zu müssen. Außerdem kann die **Beantwortung einer E-Mail-Anfrage per E-Mail eine unsichere Datenübertragungsmethode** sein. Sie birgt vor allem dann, wenn es sich um sensible Daten handelt, erhebliche Risiken. Beispiel: Eine Krankenversicherung müsste Gesundheitsdaten unter Umständen über eine unverschlüsselte E-Mail an ihre Kunden schicken. **GDV-Vorschlag:** **Art. 12 Abs. 2 Satz 3 wird wie folgt gefasst:** Die Unterrichtung hat schriftlich zu erfolgen. Stellt die betroffene Person den Antrag in elektronischer Form, ~~**ist**~~ **kann** sie **auch** auf elektronischem Weg **unterrichtet werden** ~~**zu unterrichten, sofern sie nichts anderes angibt.**~~"
3. Weigert sich der für die Verarbeitung Verantwortliche, auf Antrag der betroffenen Person tätig zu werden, unterrichtet er die betroffene Person über die Gründe für die Weigerung und über die Möglichkeit, bei der Aufsichtsbehörde Beschwerde einzulegen oder den Rechtsweg zu beschreiten.	
4. Die Unterrichtung und die auf Antrag ergriffenen Maßnahmen gemäß Absatz 1 sind kostenlos. Bei offenkundig unverhältnismäßigen Anträgen und besonders im Fall ihrer Häufung kann der für die Verarbeitung Verantwortliche ein Entgelt für die Unterrichtung oder die Durchführung der beantragten Maßnahme verlangen oder die beantragte Maßnahme unterlassen. In diesem Fall trägt der für die Verarbeitung Verantwortliche die Beweislast für den offenkundig unverhältnismäßigen Charakter des Antrags.	Um dem Antragsteller die Möglichkeit des Rückzugs seiner entgeltpflichtigen Anfrage und damit das Entfallen der Verpflichtung zur Zahlung des Entgelts einzuräumen, sollte der Antragsteller vor einer kostenauslösenden Antwort über die anfallenden Kosten informiert werden. **GDV-Vorschlag:** **Art. 12 Abs. 4 wird am Ende wie folgt ergänzt:** „**Der für die Verarbeitung Verantwortliche muss den Antragsteller vor Einleitung der Schritte zur entgeltpflichtigen Antwort über die Kosten informieren, welche dieser bei Ausführung des Antrags zu tragen hat. Dem Antragsteller muss eine angemessene Frist zur Bestätigung seines Antrags eingeräumt werden.**"

5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Voraussetzungen für offenkundig unverhältnismäßige Anträge sowie die in Absatz 4 genannten Entgelte näher zu regeln.	Der **Tatbestand des offenkundig unverhältnismäßigen Antrags erscheint ausreichend klar definiert**. Über sein **Vorliegen muss im Einzelfall entschieden werden**. Dies ist im Zweifelsfall eine Aufgabe der Rechtsprechung und **sollte daher nicht der Kommission übertragen werden**. **GDV-Vorschlag:** **Art. 12 Abs. 5 wird gestrichen.**
6. Die Kommission kann Standardvorlagen und Standardverfahren für die Mitteilungen gemäß Absatz 2, auch für solche in elektronischer Form, festlegen. Dabei ergreift die Kommission geeignete Maßnahmen für Kleinst- und Kleinunternehmen sowie mittlere Unternehmen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.	
Artikel 13 ***Rechte gegenüber Empfängern***	
Der für die Verarbeitung Verantwortliche teilt allen Empfängern, an die Daten weitergegeben wurden, jede Berichtigung oder Löschung, die aufgrund von Artikel 16 beziehungsweise 17 vorgenommen wird, mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.	

ABSCHNITT 2
INFORMATIONSPFLICHT UND AUSKUNFTSRECHT

Artikel 14 ***Information der betroffenen Person***	EG 49, 50.
1. Einer Person, von der personenbezogene Daten erhoben werden, teilt der für die Verarbeitung Verantwortliche zumindest Folgendes mit:	Die Versendung aller geforderten Mindestangaben unabhängig vom Informationsbedürfnis des Betroffenen stellt eine unnötige **Gefahr für die Sicherheit der Vertraulichkeit der Daten** dar und ist damit **in der Regel auch nicht in seinem Interesse**. Für die Unternehmen bedeutet sie einen enormen **bürokratischen Aufwand**. Die grundsätzliche Informationspflicht sollte **auf solche Informationen beschränkt sein, die der Betroffene benötigt, um weitere Auskunft erlangen zu können**. Es muss auch möglich sein, auf Verhaltensregeln nach Art. 38 zu verweisen, die die Verarbeitung der nachfolgend geforderten Informationen durch die verantwortliche Stelle regeln. **GDV-Vorschlag:** **Art. 14 Abs. 1 wird wie folgt gefasst:** „**Der für die Verarbeitung Verantwortliche teilt einer Person, deren personenbezogene Daten er erhebt oder erstmalig speichert zumindest die Tatsache der Speicherung, die Art der Daten, die Zweckbestimmung der Erhebung, Verarbeitung**

	oder Nutzung und die Identität der verantwortlichen Stelle mit.“
a) den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen sowie gegebenenfalls seines Vertreters und des Datenschutzbeauftragten,	
b) die Zwecke, für die Daten verarbeitet werden, einschließlich der Geschäfts- und allgemeinen Vertragsbedingungen, falls sich die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe b gründet, beziehungsweise die von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen, wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht,	
c) die Dauer, für die die personenbezogenen Daten gespeichert werden,	
d) das Bestehen eines Rechts auf Auskunft sowie Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen beziehungsweise eines Widerspruchsrechts gegen die Verarbeitung dieser Daten,	
e) das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,	
f) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten,	
g) gegebenenfalls die Absicht des für die Verarbeitung Verantwortlichen, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das dort geltende Datenschutzniveau unter Bezugnahme auf einen Angemessenheitsbeschluss der Kommission,	
h) sonstige Informationen, die unter Berücksichtigung der besonderen Umstände, unter denen die personenbezogenen Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten.	
2. Werden die personenbezogenen Daten bei der betroffenen Person erhoben, teilt der für die Verarbeitung Verantwortliche dieser Person neben den in Absatz 1 genannten Informationen außerdem mit, ob die Bereitstellung der Daten obligatorisch oder fakultativ ist und welche mögliche Folgen die Verweigerung der Daten hätte.	
3. Werden die personenbezogenen Daten nicht bei der betroffenen Person erhoben, teilt der für die Verarbeitung Verantwortliche dieser Person neben den in Absatz 1 genannten Informationen außerdem die Herkunft der personenbezogenen Daten mit.	
4. Der für die Verarbeitung Verantwortliche erteilt die Informationen gemäß den Absätzen 1, 2 und 3	
a) zum Zeitpunkt der Erhebung der personenbezogenen Daten bei der betroffenen Person oder	

b) falls die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, zum Zeitpunkt ihrer Erfassung oder innerhalb einer angemessenen Frist nach ihrer Erhebung, die den besonderen Umständen, unter denen die Daten erhoben oder auf sonstige Weise verarbeitet wurden, Rechnung trägt, oder, falls die Weitergabe an einen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Weitergabe.	
5. Die Absätze 1 bis 4 finden in folgenden Fällen keine Anwendung:	Die **Ausnahmen sind zu eng** und werden der **Praxis nicht gerecht**. Hier sollten zusätzlich **weitere Ausnahmen** aufgenommen werden, wie sie zum Beispiel § 33 Abs. 2 BDSG regelt. **GDV-Vorschlag:** In Ziffer 5 werden folgende Fallgruppen ergänzt: **e) „die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen oder** **f) die Daten ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten oder der verantwortlichen Stelle selbst, geheim gehalten werden müssen oder** **g) die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde oder** **h) eine Benachrichtigung dem Wohle der Europäischen Gemeinschaft oder eines Mitgliedstaates Nachteile bereiten würde oder** **i) das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden würde oder** **j) die Daten aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist oder** k) **die Daten für eigene Zwecke gespeichert sind und die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt**.“
a) Die betroffene Person verfügt bereits über die Informationen gemäß den Absätzen 1, 2 und 3 oder	
b) die Daten werden nicht bei der betroffenen Person erhoben und die Unterrichtung erweist sich als unmöglich oder ist mit einem unverhältnismäßig hohen Aufwand verbunden oder	
c) die Daten werden nicht bei der betroffenen Person erhoben und die Erfassung oder Weitergabe ist ausdrücklich per Gesetz geregelt oder	
d) die Daten werden nicht bei der betroffenen Person erhoben und die Bereitstellung der Informationen	

greift nach Maßgabe des Unionsrechts oder des Rechts der Mitgliedstaaten gemäß Artikel 21 in die Rechte und Freiheiten anderer Personen ein.	
6. Im Fall des Absatzes 5 Buchstabe b ergreift der für die Verarbeitung Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person.	
7. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten zu den Kategorien von Empfängern gemäß Absatz 1 Buchstabe f, den Anforderungen an Informationen gemäß Absatz 1 Buchstabe g, den Kriterien für die Erteilung sonstiger Informationen im Sinne von Absatz 1 Buchstabe h für verschiedene Bereiche und Verarbeitungssituationen und zu den Bedingungen und geeigneten Garantien im Hinblick auf die Ausnahmen gemäß Absatz 5 Buchstabe b zu regeln. Dabei ergreift die Kommission geeignete Maßnahmen für Kleins- und Kleinstunternehmen sowie mittlere Unternehmen.	Hier muss die **Norm selbst hinreichend bestimmt sein**. Das gilt insbesondere im Hinblick auf die in Art. 79 Abs. 5 a geregelten Sanktionen. **Für delegierte Rechtsakte ist kein Raum.** **GDV-Vorschlag:** **Art. 14 Abs. 7 wird gestrichen.**
8. Die Kommission kann Standardvorlagen für die Bereitstellung der Informationen gemäß den Absätzen 1 bis 3 festlegen, wobei sie gegebenenfalls die Besonderheiten und Bedürfnisse der verschiedenen Sektoren und Verarbeitungssituationen berücksichtigt. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.	
Artikel 15 ***Auskunftsrecht der betroffenen Person***	EG 51, 52.
1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen jederzeit eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden oder nicht. Werden personenbezogene Daten verarbeitet, teilt der für die Verarbeitung Verantwortliche Folgendes mit:	Das **Auskunftsrecht ist zu global** und äußerst unpraktikabel. Ohne eine weitere Spezifikation des Betroffenen, in welchem Zusammenhang Daten vorliegen könnten bzw. wozu genau er Auskunft wünscht, kann für die Unternehmen ein enormer Rechercheaufwand erforderlich sein. Hier ist die **Beschränkung auf einen verhältnismäßigen Aufwand geboten**. Beispiel 1: Eine betroffene Person möchte bei einem für die Verarbeitung Verantwortlichen eine grundsätzliche Aussage bekommen, ob seine/ihre Daten in irgendeiner Art und Weise gespeichert sind. Da hier der Ansatzpunkt für den Verantwortlichen fehlt (war der Betroffene Kunde, Partner, Zeuge?), müsste er seinen gesamten Datenbestand bei entsprechendem Aufwand durchsuchen. Beispiel 2: Der Kunde möchte lediglich wissen, ob eine diagnostizierte Erkrankung vom Krankenversicherer gespeichert ist. Dem Versicherer kann nicht zugemutet werden, deshalb alle aus den letzten 20 Jahren gespeicherten Daten von Krankheitskosten zu beauskunften. **GDV-Vorschlag:** **Nach Art. 15 Abs. 1 Satz 1 wird folgender Satz eingefügt:** „**Sie hat darzulegen, in welchem Zusammenhang**

	Daten vorliegen könnten, und den Gegenstand der gewünschten Auskunft genau zu bezeichnen.“
a) die Verarbeitungszwecke,	
b) die Kategorien personenbezogener Daten, die verarbeitet werden,	
c) die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben werden müssen oder weitergegeben worden sind, speziell bei Empfängern in Drittländern,	
d) die Dauer, für die die personenbezogenen Daten gespeichert werden,	
e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen beziehungsweise eines Widerspruchrechts gegen die Verarbeitung dieser Daten,	
f) das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,	
g) diejenigen personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie alle verfügbaren Informationen über die Herkunft der Daten,	
h) die Tragweite der Verarbeitung und die mit ihr angestrebten Auswirkungen, zumindest im Fall der Maßnahmen gemäß Artikel 20.	
2. Die betroffene Person hat Anspruch darauf, dass ihr von dem für die Verarbeitung Verantwortlichen mitgeteilt wird, welche personenbezogenen Daten verarbeitet werden. Stellt die betroffene Person den Antrag in elektronischer Form, ist sie auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.	Reichweite des Auskunftsanspruchs: Ein solch **weitgehender Auskunftsanspruch kann nur in Ausnahmefällen interessengerecht** sein. Dagegen ist eine detaillierte Auskunftserteilung bei Bestehen eines berechtigten Interesses des Betroffenen und der Verhältnismäßigkeit des Aufwands legitim. Hier siehe Beispiel 2 zu Absatz 1. **GDV-Vorschlag:** **Art. 15 Abs. 2 Satz 1 wird wie folgt gefasst:** „Die betroffene Person hat Anspruch darauf, dass ihr von dem für die Verarbeitung Verantwortlichen **im Rahmen ihres Auskunftsbegehrens nach Absatz 1** mitgeteilt wird, welche personenbezogenen Daten verarbeitet werden. Form des Auskunftsanspruchs: Eine elektronische Datenübermittlung birgt, insbesondere wenn es sich um sensible Daten handelt, erhebliche Risiken (dazu oben Anmerkung zu Art. 12 Abs. 2) **GDV-Vorschlag:** **Art. 15 Abs. 2 Satz 2 wird wie folgt gefasst:** „Stellt die betroffene Person den Antrag in elektronischer Form, **kann sie auch auf elektronischem Weg unterrichtet werden**, sofern sie nichts anderes angibt.“

3. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten zu den Kriterien und Anforderungen in Bezug auf die Mitteilung über den Inhalt der personenbezogenen Daten gemäß Absatz 1 Buchstabe g an die betroffene Person festzulegen.	Der spätere Erlass eines delegierten Rechtsaktes über die für die Mitteilung über den Inhalt der personenbezogenen Daten anzuwendenden Kriterien und Anforderungen bringt keinen Mehrwert für die praktische Anwendung und zeitnahe Meldung an betroffene Personen. **GDV-Vorschlag:** **Art. 15 Abs. 3 wird gestrichen.**
4. Die Kommission kann Standardvorlagen und -verfahren für Auskunftsgesuche und die Erteilung der Auskünfte gemäß Absatz 1 festlegen, darunter auch für die Überprüfung der Identität der betroffenen Person und die Mitteilung der personenbezogenen Daten an die betroffene Person, wobei sie gegebenenfalls die Besonderheiten und Bedürfnisse der verschiedenen Sektoren und Verarbeitungssituationen berücksichtigt. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.	

ABSCHNITT 3

BERICHTIGUNG UND LÖSCHUNG

Artikel 16 ***Recht auf Berichtigung***	EG 53.
Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Berichtigung von unzutreffenden personenbezogenen Daten zu verlangen. Die betroffene Person hat das Recht, die Vervollständigung unvollständiger personenbezogener Daten, auch in Form eines Korrigendums, zu verlangen.	
Artikel 17 ***Recht auf Vergessenwerden und auf Löschung***	EG 53, 54.
1. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Löschung von sie betreffenden personenbezogenen Daten und die Unterlassung jeglicher weiteren Verbreitung dieser Daten zu verlangen, speziell wenn es sich um personenbezogene Daten handelt, die die betroffene Person im Kindesalter öffentlich gemacht hat, sofern einer der folgenden Gründe zutrifft:	Die Bestimmung ist **sehr stark auf im Internet öffentlich gemachte Daten zugeschnitten**. Es sollte gründlich geprüft werden, ob die Regelung in vollem Umfang auf die Offline-Welt übertragbar ist. Beispiel: Wenn in einer Berufsunfähigkeitsversicherung Gesundheitsdaten angegeben wurden, ist die Einwilligung nach Art. 9 Abs. 2 a Rechtsgrundlage. Wird die Einwilligung widerrufen, greift Art. 17 Abs. 1 d ein und die Daten müssten gelöscht werden. Mit der Löschung ist der Vertrag nicht mehr durchführbar. (Art. 17 Abs. 1 b erfasst diesen Fall nicht, weil er sich nur auf einfache personenbezogen Daten bezieht.)
a) Die Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.	
b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz	

1 Buchstabe a stützte, oder die Speicherfrist, für die die Einwilligung gegeben wurde, ist abgelaufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung der Daten.	
c) Die betroffene Person legt gemäß Artikel 19 Widerspruch gegen die Verarbeitung ein.	
d) Die Verarbeitung der Daten ist aus anderen Gründen nicht mit der Verordnung vereinbar.	Die Bestimmung ist sehr weit (vgl. oben zu 1 geschilderten Fall). **GDV-Vorschlag:** **Art. 17 Abs. 3 wird gestrichen.**
2. Hat der in Absatz 1 genannte für die Verarbeitung Verantwortliche die personenbezogenen Daten öffentlich gemacht, unternimmt er in Bezug auf die Daten, für deren Veröffentlichung er verantwortlich zeichnet, alle vertretbaren Schritte, auch technischer Art, um Dritte, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt. Hat der für die Verarbeitung Verantwortliche einem Dritten die Veröffentlichung personenbezogener Daten gestattet, liegt die Verantwortung dafür bei dem für die Verarbeitung Verantwortlichen.	
3. Der für die Verarbeitung Verantwortliche sorgt für eine umgehende Löschung der personenbezogenen Daten, soweit deren Speicherung nicht erforderlich ist	Eine Löschung der Daten ist dann nicht gerechtfertigt, wenn sie zur Durchführung eines Vertrages oder eines gesetzlichen Anspruchs erforderlich sind (vgl. Beispiel oben unter 1.). So können z.B. Daten aus einem Haftpflichtschaden nicht gelöscht werden, wenn noch die Geltendmachung von Folgeschäden möglich ist. **GDV-Vorschlag:** **Art. 17 Abs. 3 wird um einen weiteren Buchstaben ergänzt:** „**solange die Daten noch zur Durchführung eines Vertrags oder zur Erfüllung eines gesetzlichen Anspruchs erforderlich sein können**."
a) zur Ausübung des Rechts auf freie Meinungsäußerung gemäß Artikel 80;	
b) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 81;	
c) für historische und statistische Zwecke oder zum Zwecke der wissenschaftlichen Forschung gemäß Artikel 83;	
d) zur Erfüllung einer gesetzlichen Pflicht zur Vorhaltung der personenbezogenen Daten, der der für die Verarbeitung Verantwortliche nach dem Unionsrecht oder dem Recht eines Mitgliedstaats unterliegt, wobei das mitgliedstaatliche Recht ein im öffentlichen Interesse liegendes Ziel verfolgen, den Wesensgehalt des Rechts auf den Schutz personenbezogener Daten wahren und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen muss;	

e) in den in Absatz 4 genannten Fällen.	
4. Anstatt die personenbezogenen Daten zu löschen, kann der für die Verarbeitung Verantwortliche deren Verarbeitung beschränken, wenn	
a) ihre Richtigkeit von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem für die Verarbeitung Verantwortlichen ermöglicht, die Richtigkeit zu überprüfen;	
b) der für die Verarbeitung Verantwortliche die personenbezogenen Daten für die Erfüllung seiner Aufgabe nicht länger benötigt, sie aber für Beweiszwecke weiter aufbewahrt werden müssen;	Es kann weder für Unternehmen noch für Institutionen der Strafverfolgung sowie der Finanzaufsicht von Interesse sein, dass Daten für Beweiszwecke nur im Falle bereits geltend gemachter Ansprüche weiterhin für diese Zwecke aufbewahrt werden. Die Bestimmung sollte einen entsprechenden Hinweis enthalten. **GDV-Vorschlag:** **Art. 17 Abs. 4 b wird wie folgt ergänzt:** „b) der für die Verarbeitung Verantwortliche die personenbezogenen Daten für die Erfüllung seiner Aufgabe nicht länger benötigt, sie aber für Beweiszwecke weiter aufbewahrt werden müssen**, wobei nicht erforderlich ist, dass bereits ein konkreter Anspruch geltend gemacht wurde;**
c) die Verarbeitung unrechtmäßig ist, die betroffene Person aber Einspruch gegen ihre Löschung erhebt und stattdessen deren eingeschränkte Nutzung fordert;	
d) die betroffene Person gemäß Artikel 18 Absatz 2 die Übertragung der personenbezogenen Daten auf ein anderes automatisiertes Verarbeitungssystem fordert.	In bestimmten Fällen kann die Löschpflicht wegen der Art der Datenspeicherung praktisch unerfüllbar sein. Hier ist die Aufnahme einer weiteren Ausnahme entsprechend § 35 Abs. 3 Nr. 3 BDSG geboten. **GDV-Vorschlag:** **In Art. 17 Abs. 4 wird am Ende eingefügt:** „**e) eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.**“
5. Die in Absatz 4 genannten personenbezogenen Daten dürfen mit Ausnahme ihrer Speicherung nur verarbeitet werden, wenn sie für Beweiszwecke erforderlich sind, wenn die betroffene Person ihre Einwilligung gegeben hat oder die Rechte einer anderen natürlichen oder juristischen Person geschützt werden müssen oder wenn dies im öffentlichen Interesse liegt.	Hier ist nicht ersichtlich, weshalb das Nutzungsrecht des für die Verarbeitung Verantwortlichen auf die Beweisführung beschränkt wird, während für andere Personen bereits zu schützende Rechte genügen. **GDV-Vorschlag:** **Art. 17 Abs. 5 wird wie folgt gefasst:** „**Für die Beschränkung der Verarbeitung personenbezogener Daten gemäß Absatz 4 gelten folgende Kriterien und Bedingungen:** **a)** Die in Absatz 4 genannten personenbezogenen Daten dürfen mit Ausnahme ihrer Speicherung nur verarbeitet werden, wenn **die Rechte des für die Verarbeitung Verantwortlichen oder einer anderen natürlichen oder juristischen Person geschützt werden müssen, wenn die betroffene Person ihre Einwilligung gegeben hat** oder wenn dies im öffentlichen Interesse liegt.

	[b) siehe Art. 17 Abs. 9 c unten]“
6. Unterliegt die Verarbeitung personenbezogener Daten gemäß Absatz 4 einer Beschränkung, teilt der für die Verarbeitung Verantwortliche der betroffenen Person im Voraus mit, dass die Beschränkung aufgehoben werden soll.	
7. Der für die Verarbeitung Verantwortliche trifft Vorkehrungen, um sicherzustellen, dass die Fristen für die Löschung personenbezogener Daten und/oder die regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung eingehalten werden.	
8. Wird eine Löschung vorgenommen, darf der für die Verarbeitung Verantwortliche die personenbezogenen Daten nicht auf sonstige Weise verarbeiten.	
9. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um Einzelheiten festzulegen in Bezug auf	**GDV-Vorschlag:** **Art. 17 Abs. 9 sollte aufgrund der nachfolgenden Argumente gestrichen werden.**
a) die Kriterien und Anforderungen im Hinblick auf die Anwendung von Absatz 1 für bestimmte Bereiche und spezielle Verarbeitungssituationen,	Es ist nicht erkennbar, welche bestimmten Bereiche und speziellen Verarbeitungssituationen mit Bezug zu Absatz 1 hier gemeint sind. Die gemeinten Fälle sollten wenigstens grob in Absatz 1 genannt werden. **GDV-Vorschlag:** **Art. 17 Abs. 9 a wird gestrichen.**
b) die Bedingungen für die Löschung gemäß Absatz 2 von Internet-Links, Kopien oder Replikationen von personenbezogenen Daten aus öffentlich zugänglichen Kommunikationsdiensten,	Absatz 2 definiert nicht, welche öffentlich zugänglichen Kommunikationsdienste in Absatz 9 b) gemeint sind. Auch hier ließe dies eine sehr weite Fassung der Regelung zu, die vermieden werden sollte. Daher sollten die Bedingungen für die Löschung in den genannten Fällen direkt im Absatz 2 dargelegt werden. **GDV-Vorschlag:** **Art. 17 Abs. 9 b wird gestrichen. Art. 17 Abs. 2 wird wie folgt am Ende ergänzt:** **„Hat der für die Verarbeitung Verantwortliche die personenbezogenen Daten im Internet veröffentlicht, so gelten folgende Bedingungen für die Löschung von Internet-Links, Kopien oder Replikationen von personenbezogenen Daten aus öffentlich zugänglichen Kommunikationsdiensten:** **[nachfolgend die erwähnten Bedingungen]“**
c) die Kriterien und Bedingungen für die Beschränkung der Verarbeitung personenbezogener Daten gemäß Absatz 4.	Art. 17 Abs. 4 ist hinreichend bestimmt. Es bedarf nicht der Festlegung weiterer Kriterien und Bedingungen für die Beschränkung der Verarbeitung personenbezogener Daten. **GDV-Vorschlag:** **Art. 17 Abs. 9 c wird gestrichen.**
Artikel 18 ***Recht auf Datenübertragbarkeit***	EG 55.
1. Werden personenbezogene Daten elektronisch in einem strukturierten gängigen elektronischen Format verarbeitet, hat die betroffene Person das	Die in diesem Artikel vorgesehenen Rechte können **allenfalls bei sozialen Online-Netzwerken sinnvoll** angewendet werden oder wenn Personen eigene

Recht, von dem für die Verarbeitung Verantwortlichen eine Kopie der verarbeiteten Daten in einem von ihr weiter verwendbaren strukturierten gängigen elektronischen Format zu verlangen.	Inhalte, z.B. Briefe oder Fotografien, in Cloud-Anwendungen speichern. In der Offline-Welt, wie z.B. in der Versicherungswirtschaft, ergeben sie dagegen keinen Sinn. Die Daten werden zur Verarbeitung durch die Unternehmen in deren IT-Systeme eingespeichert. **Um den Anspruch zu gewährleisten müssten die Versicherungsunternehmen ihre IT-Systeme mit einem enormen Kostenaufwand umstellen.** An einem „für ihn weiter verwendbaren strukturierten gängigen elektronischen Format“ dürfte der Versicherte kein Interesse haben. Die **Rechte der betroffenen Personen werden bereits durch das Auskunftsrecht in Art. 15 ausreichend geschützt**. Soweit eine **betriebliche Altersversorgung oder Krankenversicherung** bei einem anderen Anbieter fortgesetzt werden kann, **existieren Spezialnormen**, auf deren Grundlage die notwendigen Informationen übertragen werden. Hier bedarf es keines Anspruchs auf Übertragung sämtlicher Daten. Außerdem ist zu bedenken, dass die **Informationen für Konkurrenten oder Datenhändler von großem Interesse** sein könnten. Sie könnten die Betroffenen zur Wahrnehmung ihrer Rechte veranlassen. Dem Schutz dieser Unternehmen dient die Vorschrift aber gerade nicht. **GDV-Vorschlag :** **Um untragbare Ergebnisse zu vermeiden, muss der Artikel entweder gestrichen oder an dieser Stelle auf den Anspruch der technologischen Neutralität verzichtet werden.**
2. Hat die betroffene Person die personenbezogenen Daten zur Verfügung gestellt und basiert die Verarbeitung auf einer Einwilligung oder einem Vertrag, hat die betroffene Person das Recht, diese personenbezogenen Daten sowie etwaige sonstige von ihr zur Verfügung gestellte Informationen, die in einem automatisierten Verarbeitungssystem gespeichert sind, in einem gängigen elektronischen Format in ein anderes System zu überführen, ohne dabei von dem für die Verarbeitung Verantwortlichen, dem die personenbezogenen Daten entzogen werden, behindert zu werden.	Hiermit würde dem Kunden darüber hinaus die **Möglichkeit einer unberechtigten Kündigung eingeräumt**, indem er **durch Entzug der Daten eine Vertragsdurchführung unmöglich** macht. Die Verpflichtung, die Systeme so kompatibel zu gestalten, dass sie sich in ein anderes System übertragen lassen, dürfte nicht nur einen unverhältnismäßigen Aufwand **bedeuten, sondern auch wettbewerbswidrig sein und Geschäftsgeheimnisse gefährden**. **GDV-Vorschlag:** **Vgl. Vorschlag zu Nr. 1**
3. Die Kommission kann das elektronische Format gemäß Absatz 1 festlegen sowie die technischen Standards, Modalitäten und Verfahren für die Überführung der personenbezogenen Daten gemäß Absatz 2. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 erlassen.	

ABSCHNITT 4

WIDERSPRUCHSRECHT UND PROFILING

Artikel 19 ***Widerspruchsrecht***	EG 56, 57.
1. Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben d, e und f erfolgt, Widerspruch einzulegen, sofern der für die Verarbeitung Verantwortliche nicht zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.	Art. 6 Abs. 1 f ist eine für die Versicherungswirtschaft in der Praxis wichtige Rechtsgrundlage. Beispiel 1: Die Verarbeitung der Daten von Anspruchstellern in der Haftpflichtversicherung wird auf diese Norm zu stützen sein, weil Art. 6 Abs. 1 b nur die Verarbeitung von Daten eines Vertragspartners erfasst. Beispiel 2: Der vielfältige Einsatz von Dienstleistern, z.B. die Risikoprüfung oder Leistungsbearbeitung in einem anderen Konzernunternehmen oder der Einsatz von Gutachtern, basiert in der Versicherungswirtschaft auf einer allgemeinen Interessenabwägungsnorm. Insbesondere wenn die **Datenverarbeitung aufgrund eines Gesetzes oder der Erfüllung einer vertraglichen Vereinbarung oder sonstigen Ansprüchen darauf erlaubt** ist, kann ein **Widerspruch nur die Ausnahme** sein. Dem trägt Art. 14 der RL 95/46/EG besser Rechnung. Diese Vorschrift ist auch klarer formuliert als Art. 19 des Verordnungsentwurfs, der im Hinblick auf die Betroffenen zunächst auf „Gründe, die sich aus ihrer besondere Situation ergeben“ und anschließend auf die „Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person“ abstellen. **GDV-Vorschlag:** **Art. 19. Abs. 1 wird wie folgt gefasst:** „Die betroffene Person hat das Recht, aus **überwiegenden schutzwürdigen** Gründen, die sich aus ihrer besonderen Situation ergeben, **bei der verantwortlichen Stelle** gegen die Verarbeitung personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben d, e und f erfolgt, Widerspruch **einzulegen.**“
2. Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, hat die betroffene Person das Recht, dagegen unentgeltlich Widerspruch einzulegen. Die betroffene Person muss ausdrücklich in einer verständlichen und von anderen Informationen klar abgegrenzten Form auf dieses Recht hingewiesen werden.	
3. Im Falle eines Widerspruchs gemäß den Absätzen 1 und 2 darf der für die Verarbeitung Verantwortliche die betreffenden personenbezogenen Daten nicht weiter nutzen oder anderweitig verarbeiten.	

Artikel 20 ***Auf Profiling basierende Maßnahmen***	EG 58.
1. Eine natürliche Person hat das Recht, nicht einer auf einer rein automatisierten Verarbeitung von Daten basierenden Maßnahme unterworfen zu werden, die ihr gegenüber rechtliche Wirkungen entfaltet oder sie in maßgeblicher Weise beeinträchtigt und deren Zweck in der Auswertung bestimmter Merkmale ihrer Person oder in der Analyse beziehungsweise Voraussage etwa ihrer beruflichen Leistungsfähigkeit, ihrer wirtschaftlichen Situation, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens besteht.	Mit dem grundsätzlichen Verbot von Profilbildungen soll **in erster Linie die Bildung von Verhaltensprofilen aufgrund von Aktivitäten im Internet verhindert werden**. Die Bestimmung würde nach ihrem Wortlaut jedoch **auch automatisierte Tarifeinstufungen und Risikoeinschätzungen in der Versicherungswirtschaft erfassen**. Eine **risikogerechte Tarifeinstufung und Prämienbemessung ist aber versicherungsaufsichtsrechtlich gefordert**. Eine ordnungsgemäße Geschäftsorganisation eines Versicherers setzt nach **Art. 44 der Solvency II Rahmenrichtlinie** (RL 2009/138/EG) ein angemessenes Risikomanagement voraus, das auch die **risikoadäquate Beitragsbemessung verlangt** (dazu Stellungnahme des GDV zur Verordnung, 2.a) Beispiel: Art. 20 Abs. 1 erfasst – aufgrund der sehr weiten Definition personenbeziehbarer Daten – die automatisierte Bemessung des Beitrags danach, ob ein zu versicherndes Haus ein Reetdach oder Schindeldach hat oder ob sich ein Haus in einem Hochwassergebiet befindet. Solche Vorgänge sind für die Versicherungswirtschaft wesensnotwendig und erfolgen in Massensparten auch automatisiert. Ebenso wie der deutsche Gesetzgeber bei der ersten BDSG-Novelle von 2009 vom Scoring die Tarifierung und Risikoeinschätzung in der Versicherungswirtschaft unterschieden hat, müssen diese Vorgänge ausdrücklich vom Begriff der Profilbildung ausgenommen werden. **GDV-Vorschlag:** **Es wird nach Nr. 4 eine weitere Ziffer eingefügt.** „**Die Tarifeinstufung und Prämienbemessung zu Versicherungszwecken, die auf aktuarischen Berechnungen oder versicherungsmedizinischen Erkenntnissen beruht, wird hiervon nicht erfasst.**“
2. Unbeschadet der sonstigen Bestimmungen dieser Verordnung darf eine Person einer Maßnahme nach Absatz 1 nur unterworfen werden, wenn die Verarbeitung	
a) im Rahmen des Abschlusses oder der Erfüllung eines Vertrags vorgenommen wird und der Abschluss oder die Erfüllung des Vertrags auf Wunsch der betroffenen Person erfolgt ist oder geeignete Maßnahmen ergriffen wurden, um die berechtigten Interessen der betroffenen Person zu wahren, beispielsweise durch das Recht auf direkten persönlichen Kontakt, oder	
b) ausdrücklich aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten gestattet ist und diese Rechtsvorschriften geeignete Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person enthalten oder	

c) mit Einwilligung der betroffenen Person nach Maßgabe von Artikel 7 und vorbehaltlich entsprechender Garantien erfolgt.	
3. Die automatisierte Verarbeitung personenbezogener Daten zum Zwecke der Auswertung bestimmter persönlicher Merkmale einer natürlichen Person darf sich nicht ausschließlich auf die in Artikel 9 genannten besonderen Kategorien personenbezogener Daten stützen.	Eine **automatisierte Einschätzung aufgrund von Gesundheitsdaten, z. B. in einer schnell abzuschließenden Reisekrankenversicherung, wäre nach Art. 20 Abs. 3 generell verboten**, selbst wenn das Ergebnis für die Kunden nur positiv ist. Das Verbot der ausschließlichen Nutzung besonders geschützter Daten führt auch nicht zu einem besseren Schutz dieser. Betroffene Unternehmen könnten es durch die künstliche Hinzufügung anderer personenbezogener Daten umgehen, was für sie einigen Aufwand und für den Betroffenen keinen Nutzen bedeuten würde. **GDV-Vorschlag:** **Art. 20 Abs. 3 wird gestrichen.**
4. In Fällen gemäß Absatz 2 müssen die von dem für die Verarbeitung Verantwortlichen gemäß Artikel 14 erteilten Auskünfte auch Angaben zu einer etwaigen Verarbeitung für die unter Absatz 1 beschriebenen Zwecke und die damit angestrebten Auswirkungen auf die betroffene Person beinhalten.	
5. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Bedingungen, die für geeignete Maßnahmen zur Wahrung der berechtigten Interessen gemäß Absatz 2 gelten sollen, näher zu regeln.	Hier handelt es sich um **wesentliche Anforderungen, die in der Verordnung selbst geregelt werden müssen**.

ABSCHNITT 5
BESCHRÄNKUNGEN

Artikel 21 ***Beschränkungen***	EG 59.
1. Die Union oder die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5 Buchstaben a bis e und den Artikeln 11 bis 20 sowie gemäß Artikel 32 beschränken, sofern eine solche Beschränkung in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist	
a) zum Schutz der öffentlichen Sicherheit	
b) zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten	
c) zum Schutz sonstiger öffentlicher Interessen der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats etwa im Währungs-, Haushalts- und Steuerbereich und zum Schutz der Marktstabilität und Marktintegrität	
d) zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe	

e) für Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a, b, c und d genannten Zwecke verbunden sind	
f) zum Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen.	Diese Norm beinhaltet eine **unkalkulierbar weite Möglichkeit, die Datenschutzbestimmungen im Interesse der Betroffenen oder anderer Personen auszuweiten**. **GDV-Vorschlag:** **Art. 21 Abs. 1 f wird gestrichen.**
2. Jede Legislativmaßnahme im Sinne des Absatzes 1 muss spezifische Vorschriften zumindest zu den mit der Verarbeitung verfolgten Zielen und zur Bestimmung des für die Verarbeitung Verantwortlichen enthalten.	

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 <u>den aktuellen Stand der Technik für bestimmte Sektoren und Datenverarbeitungssituationen zu bestimmen</u>, 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 <u>situationsabhängigen</u> 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 <u>einer Verletzung des Schutzes personenbezogener Daten benachrichtigt der für die Verarbeitung Verantwortliche die Aufsichtsbehörde</u> ohne unangemessene Verzögerung und nach Möglichkeit <u>binnen 24 Stunden</u> 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, <u>das 250 oder mehr Mitarbeiter</u> 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.**

KAPITEL VIII
RECHTSBEHELFE, HAFTUNG UND SANKTIONEN

Artikel 73 ***Recht auf Beschwerde bei einer Aufsichtsbehörde***	
1. Jede betroffene Person hat unbeschadet eines anderweitigen administrativen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten nicht mit dieser Verordnung vereinbar ist.	
2. Einrichtungen, Organisationen oder Verbände, die sich den Schutz der Rechte und Interessen der betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten zum Ziel gesetzt haben und die nach dem Recht eines Mitgliedstaats gegründet sind, haben das Recht, im Namen einer oder mehrerer betroffenen Personen Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde zu erheben, wenn sie der Ansicht sind, dass die einer betroffenen Person aufgrund dieser Verordnung zustehenden Rechte infolge der Verarbeitung personenbezogener Daten verletzt wurden.	
3. Unabhängig von der Beschwerde einer betroffenen Person haben Einrichtungen, Organisationen oder Verbände im Sinne des Absatzes 2 das Recht auf Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde, wenn sie der Ansicht sind, dass der Schutz personenbezogener Daten verletzt wurde.	Ein „Verbandsbeschwerderecht“ sollte als Ausnahme zu dem Grundsatz der individuellen Betroffenheit, der einem jeden Rechtsschutzgesuch zugrunde liegt, nur unter restriktiven Voraussetzungen gewährt werden. Der Ausnahmecharakter kommt jedoch nicht zum Ausdruck. Es soll bereits genügen, dass die Institutionen in Absatz 2 der Ansicht sind, dass eine „Verletzung des Schutzes personenbezogener Daten“ vorliegt. Dieser Begriff stellt, anders als Absatz 2 und 3, nicht auf einen Verstoß gegen die Verordnung ab, sondern ist weiter und noch dazu unbestimmt. Hinzu kommt, dass nicht ausgeschlossen werden kann, dass die Aufsichtsbehörden einer Welle von Beschwerdeverfahren ausgesetzt werden, da die Möglichkeit der Beschwerde unabhängig von eigener Betroffenheit zahlreichen Akteure offen steht. Zudem könnten das Verbandsbeschwerderechte dazu führen, dass die betroffene Person ihre Rechte zwar gar nicht verletzt sieht und auch keinerlei Vorgehen gegen eine behördliche Entscheidung wünscht, ein Verband aber dennoch Beschwerde erheben kann. **GDV-Vorschlag:** **Art. 73 Absatz 3 sollte gestrichen werden.**
Artikel 74 ***Recht auf gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde***	
1. Jede natürliche oder juristische Person hat das Recht auf einen gerichtlichen Rechtsbehelf gegen sie betreffende Entscheidungen einer Aufsichtsbehörde.	

2. Jede betroffene Person hat das Recht auf einen gerichtlichen Rechtsbehelf, um die Aufsichtsbehörde zu verpflichten, im Fall einer Beschwerde tätig zu werden, wenn keine zum Schutz ihrer Rechte notwendige Entscheidung ergangen ist oder wenn die Aufsichtsbehörde sie nicht gemäß Artikel 52 Absatz 1 Buchstabe b innerhalb von drei Monaten über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat.	Mit dieser Vorschrift wird eine im Datenschutzrecht neuartige Verpflichtungsklage eingeführt. Bisher war es lediglich möglich, bei Untätigkeit der Aufsichtsbehörde nach Eingabe einer Beschwerde eine allgemeine Leistungsklage zu erheben. Da dem Betroffenen bereits umfangreiche Rechte gegenüber dem Verarbeiter zustehen, ist nicht erkennbar, dass ein Verpflichtungsbegehren aus Gründen des effektiven Rechtsschutzes erforderlich ist. **GDV-Vorschlag:** **„Jede betroffene Person hat das Recht auf einen gerichtlichen Rechtsbehelf, um die Aufsichtsbehörde zu verpflichten, im Fall einer Beschwerde tätig zu werden, ~~wenn keine zum Schutz ihrer Rechte notwendige Entscheidung ergangen ist oder~~ wenn die Aufsichtsbehörde sie nicht gemäß Artikel 52 Absatz 1 Buchstabe b innerhalb von drei Monaten über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat.“**
3. Für Verfahren gegen eine Aufsichtsbehörde sind die Gerichte des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat.	
4. Eine betroffene Person, die von einer Entscheidung einer Aufsichtsbehörde betroffen ist, die ihren Sitz in einem anderen Mitgliedstaat hat als dem, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, kann die Aufsichtsbehörde in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts ersuchen, in ihrem Namen gegen die zuständige Aufsichtsbehörde in dem anderen Mitgliedstaat Klage zu erheben.	
5. Die endgültigen Entscheidungen der Gerichte im Sinne dieses Artikels werden von den Mitgliedstaaten vollstreckt.	
Artikel 75 ***Recht auf gerichtlichen Rechtsbehelf gegen für die Verarbeitung Verantwortliche oder Auftragsverarbeiter***	
1. Jede natürliche Person hat <u>unbeschadet eines verfügbaren administrativen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde nach Artikel 73</u> das Recht auf einen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht verordnungskonformen Verarbeitung ihrer personenbezogenen Daten verletzt wurden.	Aus dem Wortlaut ist nicht erkennbar, ob das administrative Verfahren eine Art Vorverfahren zu dem gerichtlichen Rechtsbehelf darstellt. Zur Entlastung der Gerichte wäre es sinnvoll, die Zulässigkeit des gerichtlichen Rechtsbehelfs an erfolgloses und ordnungsgemäßes Vorverfahren nach Art. 73 zu knüpfen. **GDV-Vorschlag:** **„Jede natürliche Person hat ~~unbeschadet eines verfügbaren administrativen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde nach Artikel 73~~ das Recht auf einen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht verordnungskonformen Verarbeitung ihrer**

	personenbezogenen Daten verletzt wurden und das Rechtsschutzbegehren zuvor ordnungsgemäß und erfolglos bei einer Aufsichtsbehörde nach Art. 73 geltend gemacht wurde.“
2. Für Klagen gegen einen für die Verarbeitung Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, es sei denn, es handelt sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.	Damit der Gerichtsstand nicht bei sämtlichen Niederlassungen des für die Verarbeitung Verantwortlichen oder des Auftragsdatenverarbeiters begründet wird, ist es erforderlich, Einschränkungen vorzunehmen. Soweit der Betroffene nicht den Gerichtsstand seines Aufenthaltsortes wählt, bietet sich der Gerichtsstand der konkreten Rechtsverletzung, alternativ der Gerichtsstand der Hauptniederlassung an. Zudem sollte der Gerichtsstand des Aufenthaltsorts in Satz 2 nur für die Ansprüche aus der Verordnung gelten. Soweit derselbe Antrag auf Grundlage desselben Lebenssachverhalts nicht auf Basis dieser Verordnung, sondern auf einer anderen rechtlichen Grundlage (z.B.Vertrag) geltend gemacht wird, sollte diese Vorschrift nicht greifen. **GDV-Vorschlag:** **„Für Klagen gegen einen für die Verarbeitung Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter ~~eine~~ die Niederlassung hat, in der die beanstandete Datenverarbeitung stattgefunden hat, oder in dem sich die Hauptniederlassung des Verarbeitung Verantwortliche oder des Auftragsdatenverarbeiters befindet. Wahlweise können ~~solche~~ Klagen zur Durchsetzung der Rechte aus dieser Verordnung auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, es sei denn, es handelt sich bei dem für die Verarbeitung Verantwortlichen um eine Behörde, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.**
3. Ist dieselbe Maßnahme, Entscheidung oder Vorgehensweise Gegenstand des Kohärenzverfahrens gemäß Artikel 58, kann das Gericht das Verfahren, mit dem es befasst wurde, aussetzen, es sei denn, es ist aufgrund der Dringlichkeit des Schutzes der Rechte der betroffenen Person nicht möglich, den Ausgang des Kohärenzverfahrens abzuwarten.	
4. Die endgültigen Entscheidungen der Gerichte im Sinne dieses Artikels werden von den Mitgliedstaaten vollstreckt.	
Artikel 76 ***Gemeinsame Vorschriften für Gerichtsverfahren***	
1. Einrichtungen, Organisationen oder Verbände im Sinne des Artikels 73 Absatz 2 haben das Recht, die	Über Art. 76 Abs. 1 i. V. m. Art. 75 werden Datenschutzverbände zu Sammelklagen berechtigt.

in Artikel 74 und 75 genannten Rechte im Namen einer oder mehrerer betroffenen Personen wahrzunehmen.	Es ist jedoch kein Rechtsdurchsetzungsdefizit erkennbar, das derartige Klagen rechtfertigt. Das gilt im Datenschutzrecht noch mehr als im Verbraucherschutzrecht. Zur Ahndung möglicher Datenschutzverstöße gibt es – anders als z. B. bei der Überprüfung von AGB – spezielle Datenschutzaufsichtsbehörden, die nach der Verordnung umfangreiche Eingriffsbefugnisse haben. Jeder Betroffene kann sich form- und kostenlos an die Behörden wenden. Nach dem Verordnungsvorschlag soll den Datenschutzbehörden in Art. 76 Abs. 2 sogar eine Klagebefugnis verliehen werden. **GDV-Vorschlag:** **Art. 76 Abs. 1 sollte gestrichen werden.**
2. Jede Aufsichtsbehörde hat das Recht, Klage zu erheben, um die Bestimmungen dieser Verordnung durchzusetzen oder um einen einheitlichen Schutz der personenbezogenen Daten innerhalb der Union sicherzustellen.	Der Mehrwert einer behördlichen Klagebefugnis ist nicht erkennbar. Die Behörden haben zur Durchsetzung der Bestimmungen der Verordnung bereits weitgehende Befugnisse nach Art. 53. Die darauf beruhenden behördlichen Maßnahmen sind in der Regel Verwaltungsakte, die mit Bestandskraft zugleich und ohne gerichtliche Entscheidung vollstreckbar sind. Zur Durchsetzung eines einheitlichen Schutzes innerhalb der EU steht der Aufsichtsbehörden bereits die Klagebefugnis nach Art. 74 Absatz 4 zu. **GDV-Vorschlag:** **Art. 76 Abs. 2 sollte gestrichen werden.**
3. Hat ein zuständiges mitgliedstaatliches Gericht Grund zu der Annahme, dass in einem anderen Mitgliedstaat ein Parallelverfahren anhängig ist, setzt es sich mit dem zuständigen Gericht in diesem anderen Mitgliedstaat in Verbindung, um sich zu vergewissern, ob ein solches Parallelverfahren besteht.	
4. Betrifft das Parallelverfahren in dem anderen Mitgliedstaat dieselbe Maßnahme, Entscheidung oder Vorgehensweise, kann das Gericht sein Verfahren aussetzen.	
5. Die Mitgliedstaaten stellen sicher, dass mit den nach innerstaatlichem Recht verfügbaren Klagemöglichkeiten rasch Maßnahmen einschließlich einstweilige Maßnahmen erwirkt werden können, um mutmaßliche Rechtsverletzungen abzustellen und zu verhindern, dass den Betroffenen weiterer Schaden entsteht.	
Artikel 77 ***Haftung und Recht auf Schadenersatz***	
1. Jede Person, der wegen einer rechtswidrigen Verarbeitung oder einer anderen mit dieser Verordnung nicht zu vereinbarenden Handlung ein Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den für die Verarbeitung Verantwortlichen oder gegen den Auftragsverarbeiter.	

2. Ist mehr als ein für die Verarbeitung Verantwortlicher oder mehr als ein Auftragsverarbeiter an der Verarbeitung beteiligt, haftet jeder für die Verarbeitung Verantwortliche oder jeder Auftragsverarbeiter gesamtschuldnerisch für den gesamten Schaden.	Es sollte einen Gleichlauf zwischen Haftung und Verantwortlichkeit geben. Der Auftragsdatenverarbeiter handelt nach Art. 26 Absatz 2 (a) nur auf Weisung des für die Verarbeitung Verantwortlichen. Eine Haftung sollte aber nur dort greifen, wo der Auftragsdatenverarbeiter auch über die Datenverarbeitung entscheidet. Gleiches gilt für die Anordnung einer gesamtschuldnerischen Haftung mehrerer Auftragsdatenverarbeiter. **GDV-Vorschlag:** **„Ist mehr als ein für die Verarbeitung Verantwortlicher ~~oder mehr als ein Auftragsverarbeiter~~ an der Verarbeitung beteiligt, haftet jeder für die Verarbeitung Verantwortliche ~~oder jeder Auftragsverarbeiter~~ gesamtschuldnerisch für den gesamten Schaden.**
3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter kann teilweise oder vollständig von dieser Haftung befreit werden, wenn er nachweist, dass ihm der Umstand, durch den der Schaden eingetreten ist, nicht zur Last gelegt werden kann.	
Artikel 78 ***Sanktionen***	
1. Die Mitgliedstaaten legen fest, welche Sanktionen bei einem Verstoß gegen diese Verordnung zu verhängen sind, und treffen die zu ihrer Durchsetzung erforderlichen Maßnahmen; dies gilt auch für den Fall, dass der für die Verarbeitung Verantwortliche seiner Pflicht zur Benennung eines Vertreters nicht nachgekommen ist. Die Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.	Grundlage strafrechtlicher Sanktionen sollte das Ausmaß der vorwerfbaren Schuld (vgl. § 46 Abs. 1 Satz 1 StGB) sein. Der Strafe liegt zwar auch ein abschreckender Charakter zu Grunde, allerdings sollte dieser nicht vordergründig verfolgt werden. **GDV-Vorschlag:** **„(…)Die Sanktionen müssen wirksam~~,~~ <u>und</u> verhältnismäßig ~~und abschreckend~~ sein.“**
2. Hat der für die Verarbeitung Verantwortliche einen Vertreter benannt, wirken die Sanktionen gegen den Vertreter unbeschadet etwaiger Sanktionen, die gegen den für die Verarbeitung Verantwortlichen verhängt werden könnten.	
3. Jeder Mitgliedstaat teilt der Kommission bis spätestens zu dem in Artikel 91 Absatz 2 genannten Zeitpunkt die Rechtsvorschriften mit, die er nach Absatz 1 erlässt, und setzt sie unverzüglich von allen weiteren Änderungen dieser Vorschriften in Kenntnis.	

Artikel 79 ***Verwaltungsrechtliche Sanktionen***	
1. Jede Aufsichtsbehörde ist befugt, nach Maßgabe dieses Artikels verwaltungsrechtliche Sanktionen zu verhängen.	Die Befugnis zum Erlass von Sanktionen sollte sich nach den jeweiligen Zuständigkeitszuweisungen richten. Insofern bietet sich eine Klarstellung des Wortlauts an. **GDV-Vorschlag:** **„Die zuständige Aufsichtsbehörde ist befugt, nach Maßgabe dieses Artikels verwaltungsrechtliche Sanktionen zu verhängen.“**
2. Die verwaltungsrechtlichen Sanktionen müssen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Die Höhe der Geldbuße bemisst sich nach der Art, Schwere und Dauer des Verstoßes, seinem vorsätzlichen oder fahrlässigen Charakter, dem Grad der Verantwortung der natürlichen oder juristischen Person und früheren Verstößen dieser Person, den nach Artikel 23 eingeführten technischen und organisatorischen Maßnahmen und Verfahren und dem Grad der Zusammenarbeit mit der Aufsichtsbehörde zur Abstellung des Verstoßes.	Die Sanktionen sollten nur im begrenzten Maße abschreckend sein. Verwaltungsrechtlichen Sanktionen sind Ordnungswidrigkeiten und können general- oder spezialpräventiven Charakter haben. Allerdings wird das Ziel der Abschreckung stets durch das Ausmaß der vorliegenden Schuld, das die Grundlage für die Höhe der Strafzumessung bildet, begrenzt. Drakonische Strafen des Einzelnen zur Abschreckung der Mehrheit sind damit nur schwer vereinbar. Darüber hinaus sollte im Rahmen der Sanktionshöhe auch auf das Ausmaß des für den Betroffenen konkret entstandenen Schadens abgestellt werden. Insoweit bietet sich eine Anlehnung an die Formulierung des § 42a BDSG an. **GDV-Vorschlag:** „**2. Die verwaltungsrechtlichen Sanktionen müssen in jedem Einzelfall wirksam~~,~~ und verhältnismäßig ~~und abschreckend~~ sein. Die Höhe der Geldbuße bemisst sich nach der Art, Schwere und Dauer des Verstoßes, seinem vorsätzlichen oder fahrlässigen Charakter, dem Grad der Verantwortung der natürlichen oder juristischen Person und früheren Verstößen dieser Person, den nach Artikel 23 eingeführten technischen und organisatorischen Maßnahmen, ~~und~~ Verfahren und dem Grad der Zusammenarbeit mit der Aufsichtsbehörde zur Abstellung des Verstoßes und dem Vorliegen einer drohenden, schwerwiegenden Beeinträchtigung für die Rechte des Betroffenen.“**
3. Handelt es sich um einen ersten, unabsichtlichen Verstoß gegen diese Verordnung, kann anstatt einer Sanktion eine schriftliche Verwarnung erfolgen in Fällen, in denen	Für welchen Adressatenkreis eine Verwarnung offen steht, sollte anhand von nachvollziehbaren Kriterien festgelegt werden. Der sachliche Grund für die Ungleichbehandlung von großen Unternehmen im Vergleich zu Unternehmen nach Absatz 3b) ist nicht erkennbar. Ausschlaggebend sollte vielmehr das Vorliegen eines ersten, unabsichtlichen Verstoßes sein, unabhängig von wem dieser Verstoß begangen wurde. Die Verwarnung als milderes Sanktionsmittel ist Ausdruck des Verhältnismäßigkeitsgrundsatzes, auf den sich Rechtsträger unabhängig von ihrer Größe und Tätigkeit berufen können sollten.

	GDV-Vorschlag: Art. 79 Abs. 3 a und b werden gestrichen. Art. 79 Abs. 3 wird wie folgt gefasst: **„Handelt es sich um einen ersten, unabsichtlichen Verstoß gegen diese Verordnung, kann anstatt einer Sanktion eine schriftliche Verwarnung erfolgen."**
a) eine natürliche Person personenbezogene Daten ohne eigenwirtschaftliches Interesse verarbeitet oder	
b) ein Unternehmen oder eine Organisation mit weniger als 250 Beschäftigten personenbezogene Daten nur als Nebentätigkeit zusätzlich zu den Haupttätigkeiten verarbeitet.	
4. Die Aufsichtsbehörde verhängt eine Geldbuße bis zu 250 000 EUR oder im Fall eines Unternehmens bis in Höhe von 0,5 % seines weltweiten Jahresumsatzes gegen jeden, der vorsätzlich oder fahrlässig	Die in Absatz 4 bis 6 genannten Maximalbußgelder für Unternehmen sind massiv und existenzbedrohend. Die hohe Anzahl delegierter Rechtsakte in dieser Verordnung sorgt zudem für erhebliche Unsicherheiten in der Rechtsanwendung. Zahlreiche Vorschriften, deren Verletzung sanktioniert wird, beinhalten umfassende Ermächtigungen zur inhaltlichen Konkretisierung der Rechtspflichten (Beispiel: Art. 14 VII; Art. 15 II; Art. 17 IX; Art. 22 IV; Art. 23 III; Art. 30 IV). Der Bestimmtheitsgrundsatz, der nach Art. 7 Europäische Menschenrechtskonventionen auch für die EU und ihre Mitgliedstaaten gilt, verlangt, dass die Grenzen des strafbaren und bußgeldbewehrten Verhaltens erkennbar sein müssen. Sofern untergesetzliche Normen zur Konkretisierung einer bußgeldbewehrten Vorschrift herangezogen werden, muss die Ermächtigungsnorm so bestimmt sein, dass sich bereits aus ihr der relevante Tatbestand ergibt. Dieser Anforderung wird die Verordnung nicht gerecht. Denn gerade für den Fall, dass die EU-Kommission nicht oder erst später von ihren Ermächtigungen Gebrauch macht, bleibt der Rechtsanwender im Unklaren, ob seine Datenverarbeitung mit den teils abstrakten Pflichten der Verordnung übereinstimmt und setzt sich so der Gefahr einer Sanktionierung aus. Die Anforderungen an die Bestimmtheit sind umso höher, als dass die Verordnung massive Sanktionen ermöglicht. Es sollten daher Maßnahmen für eine Stärkung der Rechtssicherheit ergriffen werden. Es würde sich anbieten, die Rechtsfolgenseite für nationale Regelungen zu öffnen. Rahmenbedingungen innerhalb der Verordnung und die Anwendung des Kohärenzverfahrens würde eine einheitliche Handhabung der Sanktionen in den Mitgliedstaaten sicherstellen. **GDV-Vorschlag:** Art. 79 Abs. 4 bis 7 werden gestrichen. Art. 79 Abs. 4 wird wie folgt gefasst: **„Die Aufsichtsbehörde kann eine Geldbuße bis zu 250 000 EUR oder im Fall eines Unternehmens bis in Höhe von 0,5 % seines weltweiten**

	Jahresumsatzes verhängen. In den Grenzen dieser Verordnung legen die Mitgliedstaaten die Sanktionen fest, die bei Verstößen gegen diese Verordnung anzuwenden sind.“
a) keine Vorkehrungen für Anträge betroffener Personen gemäß Artikel 12 Absätze 1 und 2 trifft oder den Betroffenen nicht unverzüglich oder nicht dem verlangten Format entsprechend antwortet;	
b) unter Verstoß gegen Artikel 12 Absatz 4 eine Gebühr für die Auskunft oder die Beantwortung von Anträgen betroffener Personen verlangt.	
5. Die Aufsichtsbehörde verhängt eine Geldbuße bis zu 500 000 EUR oder im Fall eines Unternehmens bis in Höhe von 1 % seines weltweiten Jahresumsatzes gegen jeden, der vorsätzlich oder fahrlässig	
a) der betroffenen Person die Auskünfte gemäß Artikel 11, Artikel 12 Absatz 3 und Artikel 14 nicht oder nicht vollständig oder in nicht hinreichend transparenter Weise erteilt;	
b) der betroffenen Person keine Auskunft gemäß Artikel 15 erteilt, personenbezogene Daten nicht gemäß Artikel 16 berichtigt oder einen Empfänger nicht gemäß Artikel 13 benachrichtigt;	
c) das Recht auf Vergessenwerden oder auf Löschung nicht beachtet, keine Vorkehrungen trifft, um die Einhaltung der Fristen zu gewährleisten, oder nicht alle erforderlichen Schritte unternimmt, um Dritte von einem Antrag der betroffenen Person auf Löschung von Links zu personenbezogenen Daten sowie Kopien oder Replikationen dieser Daten gemäß Artikel 17 zu benachrichtigen;	
d) keine Kopie der personenbezogenen Daten in elektronischem Format bereitstellt oder die betroffene Person unter Verstoß gegen Artikel 18 daran hindert, personenbezogene Daten auf eine andere Anwendung zu übertragen;	
e) die jeweilige Verantwortung der für die Verarbeitung Mitverantwortlichen nicht oder nicht hinreichend gemäß Artikel 24 bestimmt hat;	
f) die Dokumentation gemäß Artikel 28, Artikel 31 Absatz 4 und Artikel 44 Absatz 3 nicht oder nicht hinreichend gewährleistet;	
g) in Fällen, in denen keine besonderen Kategorien von Daten verarbeitet werden, die Vorschriften im Hinblick auf die freie Meinungsäußerung gemäß Artikel 80, die Datenverarbeitung im Beschäftigungskontext gemäß Artikel 82 oder die Bedingungen für die Verarbeitung zu historischen oder statistischen Zwecken oder zum Zwecke der wissenschaftlichen Forschung gemäß Artikel 83 nicht beachtet.	
6. Die Aufsichtsbehörde verhängt eine Geldbuße bis zu 1 000 000 EUR oder im Fall eines Unternehmens bis in Höhe von 2 % seines weltweiten Jahresumsatzes gegen jeden, der vorsätzlich oder fahrlässig	
a) personenbezogene Daten ohne oder ohne ausreichende Rechtsgrundlage verarbeitet oder die	

Bedingungen für die Einwilligung gemäß den Artikeln 6, 7 und 8 nicht beachtet;	
b) unter Verstoß gegen die Artikel 9 und 81 besondere Kategorien von Daten verarbeitet;	
c) das Recht auf Widerspruch gemäß Artikel 19 oder eine damit verbundene Bedingung nicht beachtet;	
d) die Bedingungen gemäß Artikel 20 in Bezug auf Maßnahmen, die auf Profiling basieren, nicht beachtet;	
e) keine internen Datenschutzstrategien festlegt oder keine geeigneten Maßnahmen gemäß den Artikeln 22, 23 und 30 anwendet, um die Beachtung der Datenschutzvorschriften sicherzustellen und nachzuweisen;	
f) keinen Vertreter gemäß Artikel 25 benennt;	
g) unter Verstoß gegen die mit der Datenverarbeitung im Namen eines für die Verarbeitung Verantwortlichen verbundenen Pflichten gemäß den Artikeln 26 und 27 personenbezogene Daten verarbeitet oder deren Verarbeitung anordnet;	
h) die Aufsichtsbehörde bei einer Verletzung des Schutzes personenbezogener Daten nicht alarmiert oder sie oder die betroffene Person gemäß den Artikeln 31 und 32 nicht oder nicht rechtzeitig oder nicht vollständig von einer solchen Verletzung benachrichtigt;	
i) keine Datenschutz-Folgenabschätzung nach Artikel 33 vornimmt oder personenbezogene Daten entgegen Artikel 34 ohne vorherige Genehmigung oder ohne Zurateziehung der Aufsichtsbehörde verarbeitet;	
j) keinen Datenschutzbeauftragten nach Artikel 35 benennt oder nicht die Voraussetzungen für die Erfüllung seiner Aufgaben gemäß Artikel 35, 36 und 37 schafft;	
k) ein Datenschutzsiegel oder -zeichen im Sinne des Artikels 39 missbraucht;	
l) eine mangels eines Angemessenheitsbeschlusses oder mangels geeigneter Garantien oder einer Ausnahme gemäß den Artikeln 40 bis 44 unzulässige Datenübermittlung in ein Drittland oder an eine internationale Organisation vornimmt oder anordnet;	
m) einer Anweisung oder einem vorübergehenden oder endgültigen Verarbeitungsverbot oder einer Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 53 Absatz 1 nicht Folge leistet;	
n) entgegen den Pflichten gemäß Artikel 28 Absatz 3, Artikel 29, Artikel 34 Absatz 6 und Artikel 53 Absatz 2 die Aufsichtsbehörde nicht unterstützt, nicht mit ihr zusammenarbeitet, ihre keine einschlägigen Auskünfte erteilt oder keinen Zugang zu seinen Räumlichkeiten gewährt;	
o) die Vorschriften über die Wahrung des Berufsgeheimnisses gemäß Artikel 84 nicht einhält.	
7. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Beträge der in den Absätzen 4, 5	

und 6 genannten Geldbußen unter Berücksichtigung der in Absatz 2 aufgeführten Kriterien zu aktualisieren.	