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