

## 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](mailto:m.vomhof@gdv.de)

[www.gdv.de](http://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