Position Paper

Insurance Europe key messages on the European Commission's proposed General Data Protection Regulation

Our reference:	SMC-DAT-12-064	Date:	3 September 2012
Related documents:	Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)		
Contact person:	William Vidonja, Head of Single Market and Social Affairs, Lamprini Gyftokosta, Policy Advisor	E-mail:	Vidonja@insuranceeurope.eu Gyftokosta@insuranceeurope.eu
Pages:	7	Transparency Register ID	33213703459-54

Introduction

Insurance Europe welcomes the European Commission's (EC) objective to harmonise further the data protection legislation within the EU and strengthen individuals' rights. The EC proposed Regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data may however, have unintended consequences for insurers and consumers.

Insurers are concerned that the EC proposed Regulation will restrict insurers' ability to process and use data to properly assess risk. Collecting and processing personal data are at the core of insurance business. Being able to access and process personal data through automated processing enables insurers to process and pay claims, determine the level of cover needed, assess the risk and hence provide consumers with the appropriate premium that fairly reflects the individuals' needs and risks.

If insurers are not able to properly assess risks, there will be a significant negative impact on consumers. For example, it would prevent or delay the reimbursement of medical treatment or the compensation for car accidents, as without an appropriate assessment of the risks, insurers are unable to determine the right amounts of reimbursement or compensation. Further potential negative consequences include the increase of premiums, decrease in insurance coverage and the fact that some products may be withdrawn entirely from the market.

Furthermore Insurance Europe believes that parts of the proposal have been designed with the intention to address problems stemming from social networking, online tracking and search engine technology. These parts should not apply to other highly regulated fields of activities, to which they are not adapted, such as insurance.

Therefore, any changes to the EU data protection legislation should be relevant and proportionate, balancing the individuals' privacy right with data security, taking into consideration the way insurance works. It explicitly should recognise the need for insurers and reinsurers to process personal data in order to calculate fair premiums, and respect contract law requirements. It should also enable insurers to verify the accuracy of information provided and prevent fraud and other financial crime.

Finally, the Regulation must not overlap or be in conflict with other pieces of national or EU legislation, such as the Solvency II Framework Directive and the Anti-money laundering Directive.

Insurance Europe aisbl
rue Montoyer 51, B-1000 Brussels
Tel: +32 2 547 5811 • Fax: +32 2 547 5819
www.insuranceeurope.eu

1. Insurance specific concerns with regard to the EC's proposed General Data Protection Regulation

1.1 Consent

1.1.1 Definition of consent – Recital 25, Article 4par.8

Based on insurers' experience across member states, consumers do not encounter problems with the current rules on consent in Directive 95/46/EC. Article 2(h) of Directive 95/46/EC provides a suitable protection for the consumer without being unnecessarily burdensome, either for the consumer or for the insurer or both. The requirements of and for consent as provided by the proposed Regulation must be relevant and suitable to the purposes for which the consent is obtained. It should not prevent the insurer from delivering necessary services to the consumer.

Insurance Europe calls for the Article 2(h) Directive 95/46/EC rules on consent to be maintained.

1.1.2 Right to withdraw consent – Article 7par.3

Insurance Europe is concerned that the data subject's right to withdraw consent, as proposed by the draft Regulation, would:

(i) hinder the execution of the insurance contract: Should the consumer exercise his/her right to withdraw consent to the processing of personal data, this will give rise to serious legal problems under insurance contract law as the insurer will no longer be able to perform the contractual obligations.

(ii) lead to a cancellation of the contract because it is not foreseen by the parties: The consumer's right to withdraw consent should not result in a right of the consumer to cancel the policy. Based on insurance contract law, the insurer and the consumer fix the terms of the contract at the beginning of their contractual relationship. Some contracts permit cancellation during a given period under specific conditions. This is different from the consumer's right to withdraw consent deriving from the proposed Regulation: it was not foreseen by the parties when signing the contract and it will be perceived as a breach of the contract.

(iii) Conflict with other legal instruments: Financial service providers are required to retain data to meet legal and regulatory obligations. For example, Directive 2005/60/EC on anti-money laundering and terrorist financing, requires insurers to store data for at least 5 years after the end of the business relationship with natural or legal persons, because of public authorities' control and internal investigations amongst other reasons. National insurance legislation can also require insurers to store data for longer periods, for example 10 years in Italy and 26 years in Poland.

Insurance Europe suggests that the proposed provision on the right to withdraw consent at any time should be redesigned to take into account situations: - Where data must be retained for the conclusion and execution of insurance contracts, the settlement of a claim and - Where data must be processed for regulatory, anti-fraud or legal purposes

1.1.3 Right to be forgotten – Article 17

The EC proposal introduces the concept of the "right to be forgotten" whereby individuals can request the deletion of their personal data. Insurance Europe believes that while the intention of this requirement is to address concerns related to internet services (such as social networking sites), there is a concerning overspill to other areas where it is vital to hold data.

This is the case where there is a contractual relationship between an organisation and an individual, and data are needed for the proper performance of the contract. For example if a health insurance policyholder withdraws consent for their health data to be used or requests that information to be deleted, while this data forms an integral part of the contract, the risk assessment, as well as the assessment and processing of claims

cannot take place. This is also the case where there are regulatory requirements to retain data and where there is a need to retain data for fraud prevention purposes, as explained above.

Insurance Europe recommends that the draft Regulation is amended to clearly state that the right to be forgotten does not apply where:

- There is a contractual relationship between an organisation and an individual, and data are needed for the proper performance of the contract.
- There are regulatory requirements to retain data.
- There is a need to retain data for fraud prevention purposes

1.1.4 Significant imbalance – Recital 34, Article 7par.4

The introduction of the new term "significant imbalance" creates legal uncertainty. It could be interpreted as if there is a "significant imbalance" between insurers and consumers, in which case, the data subject's consent for processing (non) sensitive data would be invalidated and would prevent insurers from offering their services to new and existing customers.

For instance, insurers have only one legal ground to process sensitive data, that of consent. If the rule of significant imbalance applies to them, insurers will not be able to process health data anymore.

Insurance Europe calls on removing or at least amending the provision in a way that limits the unintended consequences for the insurance industry.

1.2 Health data

1.2.1 Definition of health data – Recital 26, Article 4par.12

Insurers need to process health-related data to provide certain insurance products. By way of example, health-related data for private medical insurance is processed to ensure that the consumer receives appropriate cover at a fair price for the risk that he/she poses, or to reimburse all or part of health care where the individual requires medical treatment covered by the insurance policy.

Insurance Europe believes that the definition of health data is too broad and will increase the consent requirements for certain administrative data. Treating purely administrative data as sensitive is disproportionate and will impose administrative burden on consumers and insurers. For instance, it will create delays in the pay-out of covered medical expenses which is important for insurance products that require medical data processing, for example health, motor or travel insurance.

Moreover, the indication of the patient's health problem on an accident claim or the hospitalisation admission will be considered sensitive health data and therefore the administrative employees could not process them without the explicit consent of the data subject. This, again, is burdensome for all the parties and does not provide any benefit to the data subject.

Insurance Europe calls for the definition of health data to be clear and restricted to clinical and medical information, and to exclude administrative information. Administrative information should be categorised as non-sensitive data.

1.2.2 Processing of health data – Recital 42, Article 9par.2 (h), Article 81pa.1(c)

Insurance Europe understands that insurers can process health data for the management of health care services and settling claims for the benefits and services in the health insurance system, as stated in rec.42.

However, Insurance Europe finds unclear whether insurance falls under the provisions of either Article 81 or Article 9par.2 (h). Processing sensitive data is imperative for insurers and it is crucial to clarify that the conclusion and execution of insurance contracts, including the management of health care services and settling claims for benefits and services in the health insurance system, should be permissible.

Insurance Europe calls for a confirmation of the application of either Article 9par (h) or Article 81 to the insurance or an extension of the scope for collecting and processing health data for all insurance purposes, for example health, life, accident, third party liabilities insurance and reinsurance.

1.3 Data sharing and fraud prevention - Article 6par4 and Article 9par.2(j)

Insurance Europe is concerned that changes to the EU data protection framework may have an impact on insurers' ability to share information and prevent fraud[1], which benefits honest consumers and is in the interest of the society.

Insurance Europe is concerned that the proposed Regulation will:

- Restrict insurers' ability to collect, process and use information needed for fraud prevention and detection. One of the ways insurers detect suspicious activity is by considering previous claims history (multiple claims of the same nature, multiple claims featuring same parties, etc). If they are prohibited to do so, insurers will not be allowed to protect their customers against insurance fraud whilst the majority of honest consumers will have to pay the price through higher tariffs. For instance, it is estimated that the figure for health care fraud and corruption in the EU is at least €80 million every day[2].
- Hinder the development and use of systems for the identification of fraudulent policyholders, applicants and claims which already exist in member states.

Insurance Europe suggests taking into consideration the Council of Europe (CoE) Recommendation (2002)9 on the treatment of personal data for the purposes of fraud prevention and detection as essential for the insurance activity. According to the recommendation, "actuarial activities" and risk rating are allowed; the same applies to preparing and issuing insurance covers, ie risk-based pricing and premium calculation. For this to happen, collecting and using data is indispensable.

Insurance Europe recommends that the proposed Regulation explicitly recognises the need for organisations, including insurers, to process and share information to prevent and detect fraud. This could be done through an exemption for both sensitive and non-sensitive data where processing is necessary for the purposes of preventing, detecting and addressing fraud.

1.4 Profiling – Article 20par.1

Being able to access, process and store personal data through automated processing is central to insurers' ability to provide consumers with appropriate products and services at fair prices.

There is a direct correlation between the consumers' profiled risk – as derived from multiple data used for risk assessment – and the likely claims history of a policyholder during the policy period, which, combined, determines the fair premium charged to policyholders.

Insurance Europe is concerned the proposed provision on profiling will prohibit insurers from using data effectively. This would be to consumers' detriment in the form of higher prices, lack of product innovation and/or lack of available insurance.

Insurance Europe recommends that the rules on profiling as proposed in the draft Regulation are amended to avoid prohibiting or restricting risk-adequate rating, rate classification and risk assessments necessary for premium calculation.

1.5 Data portability – Article 18

Insurance Europe believes the proposed right on data portability clearly falls outside the scope of the draft Regulation. This right deals with the use of data and not with data protection. It appears to have been created to facilitate transferring data from one social network to another.

---

[1] Country facts: According to a 2011 survey, 4% of German households admit to have committed an insurance fraud within the last five years. For non-life insurance only, the estimated loss arising from fraud is €4 billion each year. In 2010, the number of fraudulent claims in Italy reached almost 2.5% of total claims against insurers. The actual number is estimated much higher, but is difficult to detect fraud accurately. In 2010, in the UK, insurance fraud is adding on average an extra £50 a year to each UK policyholder's insurance bill. In 2011, in the NL, there were 3.371 proved cases of fraud, amounting to 29 million euros. The estimated loss from undetected fraud could add up to 150€ per family p.a. The actual number of false claims is estimated to be higher, but goes undetected.

[2] European Healthcare Fraud and Corruption Network (EFHCN)

Insurance Europe also believes the ability to change providers easily is a consumer and/ or competition issue, not a data protection one. From an insurance perspective, Insurance Europe is concerned that the proposed provision would have implications for competition and intellectual property as it may unintentionally force data controllers to disclose confidential or intellectually protected information to underwriters, eg underwriting criteria, risk and pricing tools.

Insurance Europe calls for the removal of Article 18, or at minimum, provisions should be included to adequately protect confidential and intellectually protected information.

2 General concerns with regard to the EC's proposed General Data Protection Regulation

2.1 Delegated and implementing acts

Insurance Europe is concerned that the number of delegated and implementing acts causes legal uncertainty as it is impossible to predict the final content and interpretation of key provisions[3]. The large number of delegated and implementing acts is even more worrying since the chosen legal instrument, a Regulation, is directly applicable.

Insurance Europe calls for a reduction of the number of delegated and implementing acts.

2.2 Administrative sanctions - Article 79

Insurance Europe believes the proposed sanctions for breaching the regulation are disproportionate. This is because Data Protection Authorities (DPAs) do not have discretion when deciding to impose a fine. For instance, the DPAs are obliged to impose a fine ("*shall impose a fine"*) even if the violation has not produced any damage to the data subject or if it is the first violation without considering any other mitigating circumstances.

This would lead to situations where a fine of up to 0.5% of annual worldwide turnover (which would run into millions for some insurers) will apply for responding a few days late to a request for access to personal data. Insurance Europe considers that such a sanction is disproportionate, especially where there is no impact for the individual.

Insurance Europe calls for:

- The sanctions to be defined as a competence ("may impose") and not as an obligation ("shall impose").
- A revision of the level of fines, and suggests linking their amount with the damages and harms caused by the sanctioned violation to the data subject.
- The inclusion of a provision introducing a right to appeal against the sanctions.

3 Administrative burden - Articles 31 to 34

Insurance Europe welcomes the EC's intention to reduce companies' administrative burden. However, Insurance Europe identified several proposed provisions having the opposite outcome.

3.1 Data breach notification Articles 31 and 32

Insurance Europe is in favour of a notification system with clear purposes: supporting individuals, who may have been affected to take steps to protect themselves, or allowing the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

In contrast, Insurance Europe is concerned that excessive notification requirements, as the draft Regulation proposes, could lead to consumer apathy, as has been the case in the US. Excessive notification will also distract data protection authorities from their important role of investigating serious breaches, and where necessary, taking action. This would not be in the public interest.

Insurance Europe suggests that:

- Only breaches posing significant risk of harm to data subjects - and where data subjects should take action (eg to prevent identity theft) or remain vigilant – or a serious violation of their rights should be notified

[3] Such as articles 9(3), 20(5), 6(5), 6(5), 9(3), 15(3), 17(9), 28, 31, 32, 33, 34, 81(3).

- The Regulation should not impose concrete deadlines for the notification of the data breach to the supervisory authority, but should encourage the data controller to provide a response as soon as feasible and without excessive delay.

3.2 Impact assessment and prior authorisation and consultation - Articles 33 and 34

Insurance Europe believes that the duties of assessing the impact of the envisaged processing operation imposed by Article 33 and of prior notification and authorisation of the processing of data by Article 34 are disproportionate to the objective pursued as it would lead to an extensive administrative burden.

For instance article 33par.4 and the obligation to seek the data subject's view on the intended data processing, interferes with the entrepreneurial freedom to determine its own business policy and way of processing the data. The same applies to Article 34par.2 regarding prior authorisation and consultation between the data controller and the supervisory authority before the processing of data. Moreover, Insurance Europe believes that the distinction between prior consultation and prior authorisation in Article 34 is not clear and creates legal uncertainty.

Finally, according to article 33par.7, the Commission may adopt implementing and delegating acts that will specify the criteria and conditions for the processing operations that should be included in the impact assessment. This creates further uncertainty for the insurance companies as they are not aware of the when and in what manner the impact assessment is to be made; while at the same time they are facing sanctions based on Article 79par.6(i) in case the data controller (insurance company) does not carry and impact assessment.

The impact assessment duty is also raising competition concerns:

- Article 33par.2 (e) allows each supervisory authority to list processing operations subject to an impact assessment. This means that each supervisory authority could list different operations that are subject to the impact assessment, weakening thus the impact of maximum harmonisation and creating an uneven playing field between competitors.
- The obligation to publish the assessments endangers insurers' trade secrets, and may force them to make unlawful disclosures of confidential insurance information.

Insurance Europe calls for:

- The removal of Article 33, or at least,
- Clarification of which type of data is subject to impact assessment.
- Clarifications on whether there is a difference between a prior authorisation and a prior consultation.

3.3 Information to the data subject – Article 14

The proposed provision would oblige data controllers, (eg European insurers or reinsurers) intending to transfer sensitive or non-sensitive data either to a third-country data processor (like a computing centre or other service provider) or a third-country data controller to inform every data subject (insured) of such data transfer. According to the present Standard Contractual Clauses (Processors) 2010/87/EU, such an obligation applies currently only when sensitive (e.g. health-related) data are involved.

Insurance Europe is concerned that reinsurers will not be able to meet this requirement to inform every insured of a data transfer, as reinsurers have no direct relationship with the insured persons.

Insurance Europe calls on removing or at least amending the provision in a way that excludes the unintended consequences for the insurance industry.

Insurance Europe is the European insurance and reinsurance federation. Through its 34 member bodies — the national insurance associations — Insurance Europe represents all types of insurance and reinsurance undertakings, eg pan-European companies, monoliners, mutuals and SMEs. Insurance Europe, which is based in Brussels, represents undertakings that account for around 95% of total European premium income. Insurance makes a major contribution to Europe's economic growth and development. European insurers generate premium income of over €1 100bn, employ nearly one million people and invest almost €7 500bn in the economy.

www.insuranceeurope.eu