

## CEA contribution to the European Commission consultation on personal data protection

CEA reference:	SMC-LEG-11-011	Date:	14 January 2011
ID Number:	33213703459-54		
Contact person:	William Vidonja Lamprini Gyftokosta	E-mail:	<a href="mailto:Vidonja@cea.eu">Vidonja@cea.eu</a> <a href="mailto:Gyftokosta@cea.eu">Gyftokosta@cea.eu</a>
Pages:	6		

### Summary

The CEA, the European insurance and reinsurance federation, welcomes the opportunity to contribute to the consultation on data protection and to comment on the Communication of the European Commission (EC) on “*A comprehensive approach on personal data protection in the European Union*”.

To make an informed decision, the CEA stresses the need for the EC to engage in further preparatory work assessing how the existing regulations have been functioning, and clarifying the benefits and disadvantages of continuing with the existing regulation and of a new regulation.

The CEA would like to make the following comments:

- **Risks caused by new technologies**

In its Communication, the EC highlights the risks involved in the rapid technological development, particularly with regard to online activities. When creating new rules, the EC should focus on addressing such risks. Provisions should only refer to the Internet if they are intended to counteract Internet-related risks.

- **Concept of personal data and definition under the data protection Directive**

As stated in the EC Communication (p.5), the current definition of personal data is too broad, creating confusion and giving rise to various interpretations. The restrictions proposed by the Article 29 Working Party<sup>1</sup> on the concept of personal data are not always sufficient to address this problem.

Therefore, the CEA suggests there is a need to clarify the scope of personal data, eg by specifying that legislation should not apply where there is no reasonable prospect of identifying the data subject or where the subject data cannot be identified in a reasonable period of time.

---

<sup>1</sup> Opinion 4/2007 of Article 29 Working Party.

#### ■ **Protecting sensitive data**

The EC Communication suggests clarifying the processing conditions of sensitive data in light of technological and other societal developments, and adding further categories to existing sensitive data categories. As the EC looks into this issue in more detail, any changes to existing sensitive data categories must be carefully considered. Any such additions should be made with respect to the principles outlined in Recital (54) of the directive on the processing of personal data, which states: “Whereas with regard to all the processing undertaken in society, the amount posing such specific risks (i.e. sensitive data) should be very limited”.

Secondly, further details on the precise scope of data categories that could be included are required in order to check to which extent they overlap with existing categories of sensitive data or if they are already covered by other national or European legislation. This would indeed be essential to assess the magnitude of any such change and the potential impact it can have on both consumers and the insurance industry.

For instance, if the EC wants to include genetic or biometric data in the “sensitive data” definition, it should ensure first that characteristics such as gender and age, that are visible to everyone, cannot be part of them. Only data obtained at the level of DNA, RNA and chromosome level should be covered. Otherwise the extended definition will be incompatible with the provisions of other pieces of European or national legislation.

For example, the Anti-Money Laundering Directive<sup>2</sup> (AMDL) requires insurers to collect and process numerous data such as the identity (including age and gender) and the financial information necessary to redraw the origin and destination of funds.

#### ■ **Data breach notification**

The CEA believes that if a mandatory personal data breach notification is imposed, the harm that a personal data breach poses or could reasonably pose in the future to the subject matter should be one of the main criteria that trigger the obligation to notify. If the risk of harm is limited, the benefit that the data subject will gain from the notification will be also restricted and cause unnecessary stress. It might also lead to consumer apathy, which is the case in the US where so many notifications were received that significant ones were overlooked. Finally, it would create undue administrative costs for firms and possible damage to reputation even when there is no consumer detriment.

#### ■ **Insure informed and free consent**

When examining ways of clarifying and strengthening the rules on consent, the EC should take account of the importance of tacit consent, given through concrete and unmistakable behaviours. For data flows which are necessary for the conclusion and fulfilment of the insurance contract, the instrument of consent should not be the only solution. Moreover, the voluntary nature of such declarations could at times be contested because the persons concerned need the insurance cover. Given the extent of data processing in insurance companies, systematic express consent would be burdensome. Any rule in the Directive should allow for changes in corporate structures, requiring data processing in different companies of an insurance group and the outsourcing of activities to specialised external companies or persons.

#### ■ **Sanctions**

The CEA agrees with the Commission’s approach to have effective provisions on remedies and sanctions. A risk-based approach should be adopted, focussing on areas where there is a real likelihood of serious harm to an individual or to society at large. For example, in Germany, Data Protection Authorities (DPAs) and Consumer Protection Authorities (CPAs) already have numerous possibilities of interventions and a right to take legal action is not necessary. Sanctions,

---

<sup>2</sup> Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

which are largely left to EU member states, have been massively extended; therefore the CEA sees no need for a rule at EU level. In Spain for instance, the Spanish Data Protection Agency has a very detailed sanctions regime, which offer the possibility of imposing high sanctions up to 600.000€. Nevertheless, public bodies are excluded from such sanctions and can only be subjected to public advices.

Moreover, in UK the Information Commissioners' Office (ICO) has recently acquired powers to fine and to audit public bodies (on 24 November served two organisations with the first monetary penalties). However, it is too early to say whether the ability to fine will prove adequate or whether criminal sanctions should also be introduced. It should be borne in mind that the reputational damage of a fine is likely to have a proportionately greater financial impact for larger firms.

Financial services firms should not face potential threat of double jeopardy as a result of dual regulation by the financial services regulator and the DPA. For instance, in UK, the Financial Services Authority (FSA) already has the power to impose unlimited fines and these often prove substantial – running to several million pounds.

In addition, criminal sanctions have already been considered in some national law systems of the EU Member States. Evidence from national deliberations shows that in this context, administrative sanctions are more effective than criminal sanctions. Criminal sanctions are excessive and disproportionate in relation to the data protection right violated.

- **Reducing the administrative burden**

The EC will explore different possibilities for the simplification and harmonisation of the current notification system, including the possible drawing up of a uniform EU-wide registration form. From the beginning, a mandatory notification for any personal data processing appeared to have limited benefits whereas it is useful to limit notification to “particular” processing, as is the case for Italy (see art. 37 of the Italian Code of privacy).

- **Applicable law**

The CEA agrees with the EC's approach to examine ways to revise and clarify the existing provisions on applicable law. It will improve legal clarity and give the same degree of protection to all the EU data subjects, reducing at the same time the risk of forum shopping and minimising the compliance burden imposed on firms.

For instance, in the case of cross-border data processing, the determination of applicable law might be problematic. This would be due to the differences in the implementation of the data protection directive amongst member states. This may also be due to the fact that data protection authorities apply different standards in interpreting these provisions, especially in terms of security measures that must comply the data recipient, related to the computer or paper files of personal data.

Emphasis must also be given to international privacy cooperation and we support the EC's commitment to work with the US administration and other international partners to promote a coordinated international approach to data protection. Moreover, collaboration is needed between national data protection authorities when implementing international guidelines and international data transfer rules.

- **Enhancing data control and responsibility**

The EC believes that administrative simplification should not lead to an overall reduction of data controllers' responsibility to ensure effective data protection. However, simplification is a key priority. The reduction in the administration burden should be free up data controller's resources, enabling them to focus on core compliance issues and on key activities such as establishing guidelines, helping individuals and undertakings that process data to comply effectively with data protection regulations.

- **Data protection officers (DPOs)**

The CEA would like to underline the need for clarity with regards to the EC's suggestion to appoint an independent Data Protection Officer. In particular, the CEA believes that there is a need for a clear definition of what is meant by "independent". While DPOs try to remain objective and independent, the commercial reality is that DPOs must also look for solutions that support corporate goals.

The CEA questions the mandatory character of such an appointment at European level. In many member states, such as Belgium, Germany, France, Poland and the UK, many organisations (for example, in the financial services sector) already employ DPOs. In Germany, it is common practice to appoint a DPO for insurance companies as a result of the requirement of Sect4f of the German Data Protection Act, which imposes to appoint a data protection officer on public and non-public bodies if they process personal data in an automated way.

The same applies in Poland, where it is practically mandatory for every insurance company to have a DPO. In France, the DPO is not mandatory and is to a large extent appointed by large firms. The DPO can be appointed among employees or be an independent worker. In Spain, it is not mandatory either as small and medium-size undertakings would not be able to afford it. In Belgium, the DPO is not mandatory, but its function is exercised in most insurance companies by the compliance officer.

In any case, both for member states which already use DPO and for those which do not, this envisaged provision would add new burden and costs, without any providing added value in terms of protection. This is the case for supervised sectors, which already have mandatory structures of internal audit and compliance and, optionally, a supervisory body for corporate administrative responsibility. Should the mandatory character of DPO appointment be confirmed, the EC should therefore reduce formalities related to treatments subject to authorisation.

- **Data protection impact assessment**

The EC will examine the need for an obligation for data controllers to carry out a data protection impact assessment in specific cases. This assessment is already included in the risk management activities, as well as in internal audit, in compliance and in the supervisory body for corporate administrative responsibility.

- **Data Controller (DC) and Data Processor (DP)**

The CEA would like to reiterate the importance of clarifying respective responsibilities of DC and DP. Insurers have encountered difficulty in determining the status and obligations between insurers acting as DCs and third party DPs. For instance, various member states implemented differently article 2(f) of the data protection directive: some member states generally stipulate that processors are not third parties, while others, like Germany, restrict the provision to processors established within the scope of application of the Directive.

Depending on the member state from which the third country DP operates, the requirements for admissibility concerning the transfer of data might have to be met in addition to the standard clauses of the EC. For example, IT maintenance services provided by service providers located to third countries may be significantly complicated or even excluded in the case of special categories of personal data. This, however, wouldn't have been a problem if the assignment was made from another member state.

Finally, the CEA suggests that it should be expressly clarified in article 2(9) of the data protection directive that legally dependent branches are part of the DP definition, as it reflects the prevailing concept of law.

- **Data minimisation**

The EC aims to strengthen the principle of data minimisation and to improve the modalities for the actual exercise of the rights to access, rectification, erasure or blocking of data.

The existing legislation requires the insurance industry to collect certain data in order to carry out its business, for example, the money laundering legislation requires insurers to verify the accuracy of certain personal data, eg the identity of the policyholder/ beneficiary, the origin and destination of the funds.

Subsequently, any requirement that goes beyond that in Article 6(1) (c) of the Directive (restriction to data that are relevant to the defined purpose) would not be acceptable by the insurance industry.

- **Fair processing notices (FPNs)**

The CEA agrees with the EC that data subjects should be well and clearly informed in a transparent way. However, more detail is needed on FPNs, especially it needs to be clarified whether the standard fair processing notices will be compulsory or voluntary and what type of information will be included (eg sources, uses and disclosures of data) for their standardisation. The CEA emphasises the difficulty to describe actual content in a standardised way so as to apply across all sectors and types of data processing.

- **Self-Regulation/ Codes of Conduct**

The CEA agrees with the EC's approach to promote actively codes of conduct. But where the code concerns cross-border transfers of data, there is a need to ensure that the code is accepted and registered by all relevant data protection authorities. For this purpose the CEA believes that a provision should be adopted according to which the competent national authority's assessment of compliance with the national provisions issued to implement the Directive is binding upon all supervisory authorities according to article 28 of the directive.

- **Exploring EU certification schemes**

The EC will explore the feasibility of establishing EU certification schemes in the field of privacy and data protection. A more in-depth cost-benefit analysis must be undertaken before considering EU certification schemes in the field of privacy and data protection.

- **Data sharing**

Whilst the CEA supports measures to ensure appropriate consumer protection, it is vital that the legislation recognises the need for organisations to share information in order, for example, to prevent fraud and other financial crime.

Insurers subscribe to a number of databases that are in the public good. They help, for example, to detect fraudulent activity and ensure that the premiums paid by honest policyholders are commensurate with the risk run. But in return, policyholders have to accept that they must forego some privacy by allowing insurers to share information. Moreover, policyholders will never see this as a privacy invasion, if they are informed by the insurance companies in a transparent way of the objectives of data shares, of who the data processors are and how to exercise its personal right. It is important that efforts to combat fraud which are in the overriding interests of society as a whole - where database administrators and participants respect data protection principles and rights – are not hampered by an over-zealous application of the law.

There may not be any problem related to data subjects' privacy, if the rules of anti-fraud databases are well explained and pre-defined by the data protection regulations, and if the insurance companies store and use in a responsible and transparent way.

- **Data transfers**

Should the EC decides to revise the current data protection framework the CEA would favour steps towards the harmonisation of general principles, definitions, data categories and different types of data processing. In this way, international transfers will be facilitated and National Authorities will have the freedom to define the operative aspects.



The CEA is the European insurance and reinsurance federation. Through its 33 member bodies — the national insurance associations — the CEA represents all types of insurance and reinsurance undertakings, eg pan-European companies, monoliners, mutuals and SMEs. The CEA 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 050bn, employ one million people and invest more than €6 800bn in the economy.

[www.cea.eu](http://www.cea.eu)