

## CEA contribution on the Modernisation of Convention 108

<b>CEA reference:</b>	SMC-LEG-11-033	<b>Date:</b>	10 March 2011
<b>ID Number:</b>	33213703459-54		
<b>Contact person:</b>	Lamprini Gyftokosta	<b>E-mail:</b>	Gyftokosta@cea.eu
<b>Pages:</b>	10		

### Introduction

The CEA, the European insurance and reinsurance federation, welcomes the opportunity to contribute to the consultation on the modernisation of Convention 108 that has been launched by the Council of Europe.

The CEA promotes the idea that as many countries as possible (also non-members of the Council of Europe) adhere Convention 108, so as to extend the field of equivalent legislation.

### Object and Scope of the Convention, definitions

- 1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?**

The Convention came into force before the beginning of the Internet era and the rapid developments in information and communication technologies. The technologically neutral, principle-based approach that was introduced in 1981 stood the test of time. Since technological evolution is continuous and fast, the CEA believes that the Convention should be kept technologically neutral, to avoid being out of date every time something new emerges from the field of communications and technology.

This view is also supported by the European Commission (EC) in its recent Communication on "A comprehensive approach on personal data protection in the European Union" in relation to Directive 95/46 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data". It would be prudent if the Convention, having a broader geographical and material scope than the Directive 95/46/ EC, kept the same approach.

- 2. Should Convention 108 give a definition of the right to data protection and privacy?**

-

**3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?**

According to article 3 paragraph 1, Convention 108 applies to the public as well as the private sector. The CEA thinks that this approach should be retained. For private authorities, because most of the international data traffic occurs in the private sector; and for public authorities, because they have to comply with their members states' data protection legislation when processing public files, even within their national borders.

**4. Convention 108 does not exclude of its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0)?**

It should be noted that it is not clear what the question refers to when it mentions "purely personal and household activity". If it means that the process forms part of the private or family life of a natural person, Convention 108 should exclude of its scope data processed by a natural person in the course of a purely personal or household activity, as in article 3 paragraph 2 of the Directive 95/46/EC. Members States should be prevented from deciding autonomously on this matter.

**5. The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?**

The Convention should include a definition of "processing" as in the Directive 95/46/EC where a broad set of operations performed upon personal data is included. More particularly:

*Article 2 (b) : "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".*

It would be beneficial to have consistency of approach between the Convention and the Directive in order to make the international data processing easier. This means that "collection of data", which is a key operation that marks the start of the automatic processing should be included in the definition.

Moreover, as stated in section 4.4(a) of the Recommendation No (2002) 9 "on the protection of personal data collected and processed for insurance purposes", insurance undertaking must collect personal data to issue insurance policies. For this reason and in order to clarify the normal data processing of insurance undertakings, Convention 108 should include the concept of collection of data in the automatic processing definition.

It could also be useful to include in the definition the operation of "disclosure by transmission" – that is a fundamental operation for the treatment of personal data – is part of the treatment itself, as is the case for Directive 95/46/EC and in the national legislation.

**The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?**

The Convention should include the same definition of "controller of the file" as in the Directive 95/46/EC where several criteria are listed. More particularly:

*"controller of the file" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;"*

A review of the definition of the controller of the file is desirable, especially for the facilitation of data flows within insurance groups, between direct insurance and reinsurance companies and for the shifting of tasks towards service providers.

Moreover, if the involved companies are defined as one controller of the file, the delegation and centralisation of services tasks within a group can also be facilitated. Besides, tasks have to be outsourced to competent service providers to achieve synergies and to meet the requirement of economy.

This should also be facilitated under certain legal requirements, for instance:

- if it is ensured that the data are processed only in line with the original purpose
- that the other companies have been selected carefully taking into account the appropriateness of the technical and organisational measures taken by them with respect to data protection and data security and
- if, it has been agreed in the contract that the other company offers the same guaranteed of the protection of confidential information and data protection as the insurance company itself

**6. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.**

-

## Protection principles

**7. New principles could be added to the Convention, such as the proportionality principle, which should apply to all operations carried out on the data. Such principle is also linked to the data minimisation principle which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.**

The principles of proportionality and data minimisation are already implemented in article 5 (b) and (c) of Convention 108: *“Personal data undergoing automatic processing shall be: (...) b. Stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c. Adequate, relevant and not excessive in relation to the purposes for which they are stored (...)”*.

It should be noted that the existing EU legislation requires the insurance industry to collect certain data in order to carry out its business. For example, the anti-money laundering (AMDL) 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. It is important that new provisions on proportionality and data minimisation do not hinder the fulfilment of existing requirements. In order to ensure the necessary flexibility for companies, any principles of data economy should, if possible, not be designed as an obligation, but as a target.

The insurance industry complies with these requirements. However, for the assessment and calculation of an individual risk, insurance companies need comprehensive information, so that the community of insured people is not unnecessarily put at a disadvantage due to bad risks.

**8. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or a necessary condition to a fair and lawful processing, to satisfy before any step?**

When considering consent expressed and implied, the Consultative Committee should take account of the importance of tacit consent, given through concrete 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 provision in the Convention should allow for changes in corporate structures, requiring data processing in different companies of an insurance group and the outsourcing of activities specialised external companies or persons.

The CEA understands that data subjects should be well and clearly informed in a transparent way. Nevertheless, the Consultative Committee should give more details and clarify the meaning of “*necessary condition to a fair and lawful processing that should be satisfied before any step is taken*”.

**9. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?**

Convention 108 is not compulsory as Directive 95/46/EC and this is why a detailed legitimate processing could not be efficient. Particularly with regard to a preferable accession of non EU-countries to Convention 108 a list of legitimate grounds might be too restrictive and will therefore reach little acceptance. Moreover, if the legitimate processing is defined in the convention, proportionality and tacit consent should also be included.

**10. Convention 108 does not expressly mention compatibility in relation to purpose. In today’s context personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.**

It could be useful to mention the principle of compatibility in Convention 108 in order to better clarify the limits to comply with treating personal data.

Changing the data processing goal and purpose has to be also possible, in case when an insurance company as data controller can legally justify this new purpose. For example, when law changes the data acquired by an insurance company 10 years ago may be now further processed not for the primarily goals only (eg limited to servicing the insurance processes), but may be even required for new purposed like preventing and detecting terrorism and money laundering. Additionally, the customer’s right to be additionally informed should be by definition disabled in cases when there is legal provision to process this data.

**11. Special categories of data which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime: is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?**

As the Consultative Committee looks into the issue of special categories of data in more detail, any changes to existing categories must be carefully considered. More particularly, 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 special/ sensitive data or if they are 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. Other data should only be subject to the strict safeguards if they are actually comparably sensitive.

If the Consultative Committee wants to include biological or biometric data in the “special category of data”, it should ensure first that characteristics such as gender and age, that are visible to everyone, cannot be part of them. Otherwise, the definition will be incompatible with the provisions of other pieces of European or national legislation.

For instance, the Anti-Money Laundering Directive (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 the funds. Moreover, for the conclusion of insurance contracts such as life insurance contracts, age is necessary information.

Due to the complexity of the issue and the divergencies between Contracting States, the CEA supports paragraph 48 of the explanatory report of the Convention 108 that says that *“the list of this article is not meant to be exhaustive. A Contracting State may in conformity with Article 11, include in its domestic law other categories of sensitive data, the processing of which is prescribed or restricted. The degree of sensitivity of categories of data depends on the legal and sociological context of the country concerned”*.

- 12. A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?**

The main objective should be to strengthen the media competence and data protection awareness of minors, especially if these are active on the internet – in social networks, blogs and chats – and disclose information there. If the Council of Europe takes the European Commission’s idea of an age limit into consideration, an age limit of 18 seems appropriate to ensure conformity with regulations of contract law if parents conclude an insurance contract for their child, the collection and processing of the data which are required for the proper initiation, fulfillment and settlement of the contract must remain possible.

- 13. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?**

The CEA believes that only breaches that pose a significant risk of harm to data subjects – and where the data subjects should take action (eg to prevent identity theft) or remain vigilant – should be notified. 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. A future provision might only interfere if particularly sensitive data are affected and if there is a risk of severe impairments of rights or legitimate interests of the data subjects

Experiences from the American market show that imposing on data controllers a duty to obligatory inform customers on information security breaches concerning their data processing is counterproductive and even erroneous, as it may result in information chaos and encouraging customers to set additional claims against insurance companies on these grounds.

- 14. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?**

-

- 15. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?**

The CEA believes that accountability systems are already in place and this is why a further introduction of accountability mechanisms is not necessary.

For instance in the UK, the Information Commissioner’s Office (ICO) maintains a public register of data controllers. Each register entry includes the name and address of the data controller and details about the

types of personal information they process. Individuals can check the register to find out what processing of personal information is being done by a particular data controller. Moreover, many DPAs – including the ICO – have a full suite of sanctions available to them in the event that a data controller commits an alleged breach of the legislation. This is also the case for IT and ES.

More particularly, the Spanish Data Protection Agency has the same public and private files registry which is mandatory (if not, is an infringement of the data protection regulation) for every public or private person who processes personal data and for every file that they process.

Furthermore, in ES there is a possibility of registering to Standard Code on personal protection (developed under section 27 of the Directive 95/46/EC) which should be approved by the Spanish Data Protection Agency first. It guarantees that undertakings associations or public bodies who adopt it will assume good practices, transparency, security measures and responsible use of the personal data in his data processes. The adhesion is binding for the parties, aiming at guaranteeing that members of the Standard Code comply with it.

Additionally, in the UK, the ICO has introduced a voluntary “Personal Information Promise” which is intended to help strengthen public trust and confidence in the way that organizations handle their personal information. It is a clear statement from the very top of an organization that it values the personal information entrusted to it and will put the appropriate recourses in place to look after it. It is also sends a clear signal to the workers in the organization about the importance of looking after people’s personal information and that this is something taken very seriously at senior level.

The “Personal Information Promise” does not create additional legal obligations. It reflects existing legal obligations in the Data Protection Act and puts them into straightforward language that individuals can readily understand. What it does do is to show a public commitment by the organization to comply and put in place the measures that help ensure that it complies.

**16. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?**

When introducing new technologies, every company has to ensure that these are consistent with data protection standards. In this respect, the focus should be on the objective to design programs and procedures in such a way as to ensure that data security is ensured. At the same time, requirements that put an enormous cost burden, especially on small companies which would ultimately be squeezed out of the market, should be avoided.

“Privacy by design” has already been promoted by the ICO in the UK. While it is not compulsory, privacy by design is already encouraged.

## **Rights – Obligations**

**17. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?**

The CEA believes that the data subject should have the right to access data. A right to know the source of data might be relevant to the area of advertising where data are disclosed repeatedly and where it is no possible to identify the body which originally collected the data. Nevertheless, it should be borne in mind that sometimes, the request for access can be frivolous because the data subject is only motivated by willingness to control the processing rather than to confirm the accuracy of data held. Therefore, when considering a less

limited right to access, the access to data should not cover the logic of the processing. Moreover, access to the logic of the processing should not be envisaged under Convention 108.

In the UK, it is a requirement of the 1<sup>st</sup> data protection principle (fair obtaining/lawful processing) that data subjects be told the sources (or origins) of data, as well as the uses and disclosures. Where a data controller uses a decision-making process that operates automatically and is the sole basis for any decision (eg credit scoring), the data subject is entitled if they so request to receive information as to the logic involved in the decision-making. But in disclosing this information, the data controller is not required to disclose any trade secrets.

In IT as well, the data subject has the right to obtain the indication of the logic involved in case of personal data processing carried out by means of electronic tools with prior exercise of the right of access.

In ES, access to the logic of the process is part of the access right. However, in order to prevent administrative burden and excessive cost for the data processors, the data subject must demonstrate a legitimate interest under the Spanish regulation.

**18. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.**

When the data controller processes the information legitimately under an existing exemption, the data subject should not be able to oppose the processing.

The Council of Europe should keep in mind that there are legal requirements in certain sectors which oblige the firms to collect certain data as proof of financial status. The right of opposition could be introduced as in Directive 95/46/EC when permit data processing.

The same reasoning will occur with the right to oblivion since the data should be kept by firms until the end of the contract and for legal purposes (eg keeping a document as a proof for potential litigation) or legal duties to preserve records, such as according to regulations of commercial and tax law. A right of oblivion may be addressed, if at all, in connection with the use of social networks on the internet.

Data should be kept for as long as it is relevant and for evidential purposes. This period will often be linked to the statute of limitations in each member state.

**19. Should there be a right to guarantee the confidentiality and integrity of information systems?**

-

**20. Should a right "not to be tracked" (RFID tags) be introduced?**

-

**21. Should everyone have a right to remain anonymous when using information and communication technologies?**

-

**22. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0.)?**

-

## Sanctions and Remedies

### **23. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?**

The CEA believes that class actions should not be introduced in the Convention. The nature of these sanctions and remedies should be determined by member states' national legislation. But, in any event, it should be borne in mind that earlier this month, the European Commission (EC) launched a consultation about adopting a more coherent approach to collective redress by identifying common legal principles. The EC is exploring whether collective redress should be extended to new sectors. We suggest that any consideration of whether class actions should be introduced into Convention 108 would need to be discussed in the context of the EC consultation.

Class actions make sense only if no data protection authority is designated and no other protective mechanisms exist. For instance, supervisory authorities according to Directive 95/46/EC have extensive powers, and may act not only upon requested of data subject but also ex officio.

It should be borne in mind that the European Commission launched a consultation about adopting a more coherent approach to alternative dispute resolution (ADR) mechanisms by identifying common legal principles. This is why the CEA believes that any discussions related to ADR should be discussed in the context of the EC consultation.

In the offline area instead, out-of-court possibilities for dispute settlement should be developed as a matter of priority. For instance, the German insurance industry has gathered positive ombudsman for insurance, a neutral and independent arbitration board, which works free of charge for the consumer and enjoys wide acceptance among customers.

## Data protection applicable law

### **24. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?**

Given the increased complexity caused by globalization and technological advances (eg cloud computing) the CEA believes that there is a need to clarify requirements around applicable law. This is necessary, not least to reduce risk of forum shopping and the compliance burden imposed on firms.

Especially, in case of cross-border data processing, the determination of applicable law might be problematic. At EU level, 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 with the data recipient, related with the computer or paper files of personal data.

One of the revised Convention 108 must be solve this problem of applicable law to data processing, by promoting the international cooperation and guidelines on data protection issues and rules between the countries.

## Data Protection Authorities

### **25. How to guarantee their independence and ensure an international cooperation between national authorities?**

-

**26. Should their role and tasks be specified?**

The CEA does not support this suggestion as this matter falls within the national authorities; responsibilities. Their role and tasks must be addressed by the national rules and regulations of each data protection authority.

**Transborder data flows**

**27. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.**

The CEA favours steps towards the facilitation of international transfers and free flow of information regardless of frontiers by Convention 108, as it is enshrined in Article 10 of the European Human Rights Convention. As it is enshrined in Article 10 of European Human Rights Convention, the international transfer of data should assume the same level of protection from a country to another one.

Personal data protection is equally important to the correspondents of MTPL insurers, the Green Card Bureaux, Motor Guarantee Funds and Compensation Bodies, which handle insurance claims on a daily basis and which must transfer personal data in an international context in order to meet with their responsibilities.

**28. Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?**

It would be important and useful to promote codes of conduct concerning cross-border transfers of data, ensuring that every code is accepted and registered by all relevant data protection authorities. It will also be very useful to establish minimum international rules of international data transfers, especially in the insurance market, which have a continuous data flow and can operate in many countries at the same time and must comply with very different data protection legislations.

The Consultative Committee should take into account section 12.2 of Recommendation 2002 No 9, relating to "transborder data flows" which states that the insurance undertakings, which belongs to Contracting States of Convention 108, and are from countries that guarantee an adequate level of protection, must not be imposed to special conditions of privacy related to "transborder data flows".

**29. Should there be different rules for public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?**

The CEA believes that the legislation should be applicable equally to both public and private sectors. However, national DPAs should have the right to consider whether these sectors should be treated differently in certain circumstances. By the way of example, in the UK, the Information Commissioner adopts a different approach to auditing of public bodies (compulsory) and private bodies (consensual).

Moreover, Convention 108 may foster the resource to ethic codes, above all in case of multinational groups. However, it should be noted that any violation to data protection can be exclusively ascribed to the company exerting the violation unless a provision by a national law or an agreement between the parties be envisaged.

Already according to Directive 95/46/EC, the stipulation of BCR is a way to legitimise international data flows. An important aspect is the practicability of authorisation procedures. This includes recognition of the

authorisation granted by one data protection authority by other authorities to avoid multiple cost-intensive and time-consuming inspection effort.

### Role of the consultative committee

**30. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?**

Should the role of the consultative committee be strengthened, this should only be in relation to monitoring functions.

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.