

Council of Europe consultation on the modernisation of Convention 108

9 March 2011

This paper is submitted on behalf of EFAMRO, the European Federation of Associations of Market Research Organisations and ESOMAR, the World Association of Research Professionals.

Founded in 1992, EFAMRO represents the interests of market, social and opinion research in Europe. Its members are national trade associations for research businesses.

Founded in 1948, ESOMAR gathers together nearly 5000 individual members worldwide on both the provider and client side as well as in public bodies and academic institutions.

Introduction

EFAMRO and ESOMAR welcome the opportunity to respond to the Council of Europe's consultation on the modernisation of Convention 108. We have consulted with key stakeholders in the market, social and opinion research sector not only in Europe but across major global markets in the preparation of this response. We confirm that the contents of this paper are not confidential and can be attributed to EFAMRO and ESOMAR.

We note that the 30 consultation questions cover many topics with potential impact for our sector and due to the relatively tight response deadline we have concentrated on the topics which appear, at this stage, to be of the most particular concern to the research sector. It should be noted that we are interested in the whole of the data protection consultation and would wish to be involved in any of the broader discussions that the expert committee set up under Convention 108 (the T-PD) will hold, not just the topics which are covered in this response.

Market, social and opinion research

Research in itself does not seek to change or influence opinions or behaviour. Unlike direct marketing, advertising or other commercial communications, it does not seek to promote the aims or ideals of those who conduct or commission it. While research is used by marketers to test their products or messages, it is not a commercial communication.

Market, social and opinion research plays a key role in helping businesses and other constituencies better understand consumers, customers and citizens in developing goods and services and is essential for economic efficiency, innovation and progress. Social and opinion research is widely used by public bodies to understand citizens' preferences and measure key performance indicators, for example the Eurobarometer surveys carried out by the European Commission, and government studies used for improving educational, healthcare and police services.

Market, social and opinion researchers adhere to self-regulatory codes of conduct covering a range of data protection and privacy issues. Since the 1940s, market, social and opinion research has been robustly self-regulated by a family of codes of conduct and practice, supported by strong compliance and disciplinary frameworks. Amongst these, the ICC/ESOMAR International Code on Market and Social Research (last updated 2007) is used in 17 EU Member States and 58 associations in 47 countries internationally.

The fundamental principles of research, shared by the ICC/ESOMAR International Code and other codes used by national associations are that:

- Research must be conducted with the voluntary cooperation of respondents, based on the principle of informed consent.
- Respondents must not be harmed or disadvantaged as a result of participating in a research project.
- Personal data collected for research purposes must not be used for other purposes.

These principles mirror those of Convention 108. We also note that the Council of Europe has developed similar conditions which apply to research in its Recommendation No. R(97) 18 (hereafter "R(97) 18") concerning the protection of personal data collected and processed for statistical purposes. ESOMAR raised this issue with the T-PD in 2010 during the development of the *Recommendation On The Protection Of Individuals With Regard To Automatic Processing Of Personal Data In The Context Of Profiling*. Data collected and processed for statistics are already subject to more detailed provisions in R(97) 18. The Recommendation covers a number of issues raised in the current consultation's questionnaire, including consent, sensitive data, rendering data anonymous, rights of access, communication of data for non-statistical purposes, conservation of data for research quality checks, rules for transborder data flows and security of personal data. In particular, we note the following points are recognised by R(97) 18:

- Research assists both public and private bodies in decision-making and promotes the advancement of knowledge.
- Research is valuable whether carried out by public or private/commercial bodies. Research by commercial organisations should not be treated differently than research by public bodies (the latter which we would understand to include universities etc.)

- Research results designed to “characterise a collective phenomenon” mean that the emphasis is not placed on the significance of the individual’s personal data. The Convention should recognise the fundamental distinction between the individual use of personal data and their collective use.
- Paragraph 14. b. of the Explanatory Memorandum of R (97) 18 notes that “every effort is made to ensure the least possible disruption for the individual through the actual gathering of the information.” Research codes of conduct require that data collection is relevant and not excessive and, further, that individuals are protected from harm or adverse consequences of participating in a research project.
- Data collected for research purposes must only be used for research and not used or communicated for other purposes. This is also a key requirement in market, social and opinion research codes of conduct and guidelines.
- Processing of data for research is systematically followed by a quality control back-checking phase, therefore automatic processing of information which identifies individuals can legitimately also be used for the related purpose of quality control.

Our numbered responses correspond to the question numbers in the consultation document.

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?

While EFAMRO and ESOMAR would support provisions that relate to specific organisational measures, we do not believe that the revised Convention should contain specific technological provisions, as this would impair its technology neutral status.

A technologically neutral approach remains relevant. Similar to Directive 95/46/EC, the Convention sets out principles that are independent of media or techniques. This provides flexibility in allowing for the interpretation of the principles appropriate for each platform or technique. It also provides a role for self-regulation. In the context of market, social and opinion research, codes of conduct and guidelines are regularly reviewed and adapted quickly to reflect social or technological developments. These support the necessary and ongoing re-interpretation and application of the principles in a rapidly changing technological environment.

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 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?

EFAMRO and ESOMAR recommend that collection should not be subject to a special provision, but rather included in the definition of processing in the Convention. This would align the Convention with Directive 95/46/EC which includes collection as part of “processing” in 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, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

Convention 108 also differs from Directive 95/46/EC as it defines the controller as the person who determines the purpose of the automated data file, rather than the EU's definition of the controller as the person who determines both the means and the purpose of the processing of personal data.

The preferred solution would be to harmonise these definitions. In our submissions to the European Commission, we have advocated for the introduction of a clarified definition of data controller which would place responsibilities on those who decide how data are processed as opposed to those who control a particular computer or filing system.

This would restate the responsibility of a single data controller to assess the need to process personal data and the security of such systems before electing to process personal data in them and would provide a single point of responsibility and accountability to citizens. Since the operator of a particular computer or filing system would be contractually bound or otherwise obliged to abide by their representations about system integrity to those who use their systems for processing data, there is no disruption to the continuity of data protection.

A clarified definition of data controller would also restate the responsibility of data controllers to assess the security of such systems before electing to process personal data in them. Clarification of this definition would furthermore serve to increase harmonisation across the Member States.

In the market, social and opinion research context, data may be processed by a telephone centre, a website and by research analysts as part of the same project. Each section or part may work within separate entities and hold data in separate systems. Process standards (such as ISO 20252¹ and similar national standards) and ethical standards (codes of conduct and practice) ensure that each aspect is managed consistently and that respondents are protected. A single data controller assists the protection of individuals as there is a single point of responsibility and accountability. The phenomenon of multiple controllers decentralises this function and increases the risk of errors occurring.

¹ ISO 20252:2006 establishes the terms and definitions as well as the service requirements for organizations and professionals conducting market, opinion and social research.

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

Further to our response to question 5 above, EFAMRO and ESOMAR do not believe that new definitions are necessary for processors or manufacturers of equipment. The primary responsibility for the protection of personal data should rest with the data controller. Data controllers should be free to make properly informed decisions about the processors or technology they use.

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 a 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.

EFAMRO and ESOMAR believe that the emphasis in the Convention should be on responsible data collection and data minimisation, retaining data only where it is necessary for the purpose for which it is collected.

In research, the International Standard for market, social and opinion research, ISO 20252, the development of which was strongly supported by EFAMRO and ESOMAR, sets down retention periods for data collected or generated in the course of research projects and this is also reflected in the sector's self-regulatory codes. The purpose of these retention periods is to allow for necessary processes such as quality control and verification of results. These are essential activities to ensure research is robust and representative, and undertaken whilst balancing this with not keeping data longer than is necessary once the process has been fulfilled. The Convention should support and encourage the development of such policies and practices by data controllers.

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

EFAMRO and ESOMAR believe the requirement for unambiguous consent is sufficient as currently exists in the EU Directive 95/46/EC but should be clarified for consistency of application. Unambiguous consent requires data subjects to clearly be informed about the data that is being collected about them, who will have access to it and what it will be used for. We consider this level of consent to be sufficient to ensure that data is adequately protected.

In many cases, unambiguous consent is obvious – in research a respondent to a research project provides the answers to the questions they are asked, having been informed of the identity of the researcher, the purpose of the interview, and of their right to withdraw at any time. There is no specific question to obtain permission for the processing of data, but the consent of the data subject is unambiguous nonetheless from the circumstances of the data collection.

Only in cases where data processing is not obvious or where further processing is intended at a later date would additional information need to be provided and consent obtained by the asking of a specific question. The interpretation of explicit consent has varied from jurisdiction to jurisdiction and should not be interpreted as written consent as this would introduce a disproportionate administrative burden and hamper the collection of responses for market, social and opinion research. For example, in Europe, telephone research is an essential tool in discovering and understanding the views of hard-to-reach groups, such as geographically isolated communities, individuals with disabilities, or the elderly. A requirement for written consent, not possible in telephone communications, would deprive these respondents of their right to be heard, and deprive research users' access to important research findings.

An over-emphasis on consent has led to a distortion of the concept as it is used in a one-size-fits-all approach. Insisting on explicit consent for every data collection event and not just sensitive data events will embed an "always click yes" mentality in data subjects. By treating all consent in a formulaic way the value of consent overall is diminished and may in fact mean that data subjects are less protected. Further, requiring explicit consent in all cases would place disproportionate burden on both the data subject and the data controller. Such a burden is restrictive and not enabling – it impedes the flow of data without a commensurate increase in the protection of the rights of the data subject. For research, requiring explicit consent for every data collection event would reduce response rates and levels of unbiased results and thus the possibility to achieve accurate sampling on which quantitative research is based. The fundamental principles of research, shared by the ICC/ESOMAR International Code and other codes used by national associations are that research must be conducted with the voluntary cooperation of respondents, based on the principle of informed consent.

If the question of consent is considered for inclusion in Convention 108, then this should be informed by current discussions on the revisions of Directive 95/46/EC. Consent is currently considered at EU level as the first of six conditions set out in Directive 95/46/EC for fair and lawful processing in Article 7. Current EU rules have generated a lack of clarity about the other five grounds for fair and lawful processing currently in Article 7.

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?

EFAMRO and ESOMAR would welcome the introduction of a ground for legitimate processing in Convention 108. We would not support an exhaustive list of legitimate grounds for data processing.

If the Convention decides to include a provision on allowing processing where it is necessary for the purposes of the legitimate interests pursued by the controller as the EU currently does in article 7, a harmonised approach would be necessary. We would note that processing data for market, social and opinion research does not directly affect the rights or freedoms of the data subject (indeed by giving citizens a voice, research strengthens the democratic rights and freedoms of European data subjects). We believe that this condition can be appropriately

applied, for example, to the use of publicly available information to form robust and reliable sample frames for research.

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.

In the revision of the Convention, market, social and opinion research should not be considered as incompatible with the initial purpose of the data collection. This is already recognised in the R(97) 18 subsequent to the Convention and in Directive 95/46/EC Article 6, paragraph 1.b)

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered incompatible provided that Member States provide appropriate safeguards.

EFAMRO and ESOMAR recommend that a similar provision is introduced in a revised Convention.

Market, social and opinion research supports decision-making and this research in itself does not seek to change or influence opinions or behaviour. The fundamental principles of research, shared by the ICC/ESOMAR International Code and other codes used by national associations are that personal data collected for market, opinion and social research must not be used for other purposes. This in turn limits all processing of the data, and the extent to which it may be further processed and accessed.

Once collected for research, data relating to identifiable individuals may be processed further as part of quality control and verification. This protects the robustness of research results by ensuring for example that individuals or groups of individuals cannot bias research projects by submitting multiple or fraudulent responses. As more research moves to online environments, this kind of processing will become more necessary to guarantee the quality and robustness of European research and statistical data, vital to the development of the European economy and as such should be recognised as a legitimate purpose. We would note that R(97) 18 recognises that "identification data used as ancillary data" is an integral part of the production of statistical results.

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.?

We do not see the need to add other categories of data to the list of sensitive data and recommend that these should be harmonised with the EU Directive. However, we consider that additional clarity regarding the scope of what constitutes sensitive data would make compliance simpler.

As an additional point, we are aware that in some countries, data protection supervisory authorities are required to give their prior consent before sensitive personal data can be obtained from data subjects. The differences in the way that additional safeguards are applied by domestic authorities to special categories of data hampers the conduct of market, social and opinion research and does not add to the protection of individuals.

EFAMRO and ESOMAR believe that obtaining the free and explicit consent of the data subject for the processing of this information offers sufficient protection and control to the data subject. Further requirements of third-party authorisation of the data collection would place an unwarranted burden on research and its ability to produce robust and valid data for the benefit of European businesses, governments and citizens.

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 Convention does not explicitly contain provisions for the protection of children; nevertheless many sectors including market, social and opinion research have actively introduced additional rules to ensure the adequate protection of children and young people who are not yet adult. This includes all the relevant self-regulatory research codes in Europe. The protection of children and young people should not be over-simplified to a mandatory requirement for parental or guardian consent for contact with all individuals under 18 nor should children's data be classified as sensitive data in the revised legislation to reflect this consideration.

Persons under 18 may leave school, or attend university and are autonomous persons. The UN Convention on the Rights of the Child also guarantees right to express views to participate in society:

Article 12: States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.

Article 13: The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.

If additional measures were to be introduced, the need to address concerns for the protection of children and young people must be balanced with their rights of expression. Children have the ability to take decisions that are appropriate to their competence, environment and corresponding to their age, whilst noting for example it would not be appropriate to expect a child to take transactional decisions usually taken by the head of the household.

We recommend that if additional restrictions were to be introduced that these mirror the self-regulatory rules already in place, the majority of which require consent or supervision of a responsible adult such as a parent or guardian with under 14s. It is our view that if we are to properly prepare children and young people for the transition from childhood to adulthood that the transition should start at 14 not 18. For those over the age of 14, it is generally accepted that they can provide personal information for research as a young person can make an informed decision and take into account the consequences of providing that information which does not involve a personal obligation.

This will depend on the sensitivity of the survey topic. Existing self-regulatory rules and guidelines require researchers to seek parental consent on more sensitive topics providing this does not conflict with the interests or rights of the young person.

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?

EFAMRO and ESOMAR support enabling citizens to decide how and when their personal data should be collected and processed. This is reflected both in the fundamental principles of research and in the practical application of research codes of conduct and practice. Privacy and data protection should be a key design consideration in the development and application of new information technologies. Examples include:

- Default settings in social networking sites that protect privacy while allowing citizens to choose lower levels of privacy if they wish;
- Transparent, understandable and comprehensive privacy policies that provide citizens with information that they need to know before their personal data are collected and processed.

EFAMRO and ESOMAR support the principle of privacy by design forming part of the technical and organizational measures required to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing. This is particularly important where the processing involves the transmission of personal data over a network.

The application of this principle should however allow for relevant and necessary use of information in relation to the risks of the technology used. The application of the principle should also be technology neutral. New technologies should not be subject to either a higher or lower standard of scrutiny than technologies in current use. This would inhibit the development of new technologies necessary for the development of the EU economy and of innovation in the research sector.

There is a need for greater understanding and appreciation of current privacy and data protection practice in the design and application of new technologies before specific new requirements are put in place. This is necessary to

avoid discouraging technological development; the Convention should strive to encourage innovation while protecting the rights of citizens.

Code holders, trade bodies and other organisations can encourage this protection by ensuring that privacy and data protection features are designed into new developments and form part of the compliance framework for that sector. In research, EFAMRO and ESOMAR already require this of their members.

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.

As we have noted above, research must be conducted with the voluntary cooperation of respondents, based on the principle of informed consent. This provides individuals with a natural right of opposition to data processing for research purposes. Further, data relating to identifiable individuals is generally held on a time-limited basis by research companies, so respondents are soon “forgotten” by research organisations. A possible exception to this is access panels, which hold data on individuals who have volunteered to be selected for a variety of research projects. These panellists may of course choose at any time to withdraw from the panel and have their personal data removed.

EFAMRO and ESOMAR believe that both these concepts (of opposition and to be forgotten) are included in the current principle of data minimisation. The articulation of these rights would not change the current status for research, but should be expressed in such a way that they offer additional clarity to data controllers and data subjects on the lawful and fair processing of data.

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

EFAMRO and ESOMAR support the clarification of the definitions of the terms used in the principles and the harmonisation of their application across the Member States. The process of harmonisation should however seek to understand current divergences in interpretation to ensure that no single national market or jurisdiction is disproportionately affected by a change in the application of the Data Protection Directive.

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?

“Transborder data flow” is a problematic concept with little practical application to the modern internet, distributed computing and global business organisations. EFAMRO and ESOMAR see this as a further reason to

strengthen and clarify the role of the data controller to ensure that they fully consider and address the protection and security of personal data before they elect how the data will be processed.

29) Should there be different rules for the 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 public and private sectors should operate under the same rules. Given that large scale public research, including the Eurobarometer depends on the expertise of private sector organisations, and that many European economies are depending on the private sector to stimulate future economic growth, such a differentiation would be unreasonable.



For further information on EFAMRO and its activities, contact Barry Ryan, Director of Policy & Communication.

EFAMRO

Bastion Tower, level 20
Place du Champ de Mars 5
B-1050 Brussels
T : +32 (0)2 550 3548
F : +32 (0)2 550 3584
E : barry.ryan@efamro.eu
W : www.efamro.eu



For further information on ESOMAR and its activities, contact Kathy Joe, Director Professional Standards and Public Affairs.

ESOMAR

Eurocenter 2, 11th floor
Barbara Strozziilaan 384
1083 HN Amsterdam
The Netherlands
Tel: +31 20 664 2141
Fax: +31 20 664 2922
E : public.affairs@esomar.org
W : www.esomar.org