

ESOMAR WORLD RESEARCH CODES & GUIDELINES

NOTES ON HOW TO APPLY THE ICC/ESOMAR INTERNATIONAL CODE OF MARKETING AND SOCIAL RESEARCH PRACTICE



All ESOMAR world research codes
and guidelines, including latest updates,
are available online at www.esomar.org

Copyright © ESOMAR 2001

Last revised: 2001
Latest reprint: 2005

ESOMAR WORLD RESEARCH CODES & GUIDELINES

NOTES ON HOW TO APPLY THE ICC/ESOMAR INTERNATIONAL CODE OF MARKETING AND SOCIAL RESEARCH PRACTICE

CONTENTS

Introduction	2
Specific notes	2
Annexe to notes on the ICC/ESOMAR International Code of Marketing and Social Research Practice 2001 European Union Data Protection Requirements	16

ESOMAR WORLD RESEARCH CODES & GUIDELINES

NOTES ON HOW TO APPLY THE ICC/ESOMAR INTERNATIONAL CODE OF MARKETING AND SOCIAL RESEARCH PRACTICE

INTRODUCTION

These Notes are designed by ESOMAR to help users of the International Code to interpret and apply it in practice. Any further questions about the Code, for example on how to apply it in a specific situation, should be addressed to the Secretariats of ESOMAR or the ICC, as appropriate.

The Notes will be reviewed periodically to take account of changing circumstances or important new issues. When necessary, further editions will be published by ESOMAR after consultation with the ICC and with other relevant bodies.

The ICC has also published other Codes of Practice which cover a variety of marketing issues not addressed in the ICC/ESOMAR International Code. In particular, the ICC's Code on Direct Marketing deals with the different requirements which apply to that separate field of marketing activity.

SPECIFIC NOTES

SECTION A: GENERAL

Rule 2 This Rule requires that researchers must always conform to the requirements of international and national legislation. Whenever national or international law imposes obligations in any given country which are more

onerous than those already imposed by the ICC/ESOMAR Code, as elaborated in these Notes, researchers must comply with these stricter obligations.*

One very important element of legislation relates to data protection. The European Data Protection Directive, and the national legislation stemming from it, sets out the requirements which must be complied with by researchers based or carrying out research in the EU, or handling personal data collected within the EU. The key implications of such legislation for marketing research, including social and opinion research are covered in the present Notes. However, for more detailed guidance on what is required by the Directive when dealing with research in the EU, readers are referred to, and must comply with, the special ESOMAR "Annexe to Notes on the ICC/ESOMAR International Code" which describes the EU Data Protection requirements. Where researchers have questions on detailed local issues they should also refer to the relevant national marketing research associations for further advice on current national data protection requirements in the countries in which they plan to carry out research.

Marketing research conducted according to the principles of transparency,

confidentiality and secure handling of personal data has achieved growing recognition as a form of “statistical or scientific research” since personalised information cannot be disclosed for non-research purposes such as direct marketing. This guarantees the confidential nature of marketing research data. Such recognition must not be jeopardised by any failure to conform to these principles.

SECTION B: THE RIGHTS OF RESPONDENTS

All respondents are entitled to be sure that when they voluntarily agree to cooperate in a marketing research project they will be fully protected by the provisions of the ICC/ESOMAR International Code, as elaborated by these Notes, as well as by the relevant provisions of national and international law. This applies equally to respondents interviewed as private individuals and to those interviewed as representatives of organisations of different kinds.

The EU Data Protection Directive covers only “personal data”, defined as information relating to identified or identifiable natural persons. An “identifiable person” is someone whose identity can be determined either directly (for example by name, address

or identity number) or indirectly by information concerning the person’s physical, physiological, mental, economic, cultural or social characteristics. This includes audio and visual material such as tapes, film or video recordings.

The Directive requirements mean inter alia that in their dealings with the public researchers must collect, process and use all personal data “fairly and lawfully”; be transparent in their explanations to respondents of how their personal data will be handled and used; not place undue burdens on respondents; and apply adequate safeguards to ensure the security of any personal data they collect unless and until it is made impossible to identify the data subject (i.e. the respondent) and the data have therefore ceased to be “personal data”. The requirements of national legislation may vary from country to country but the undertaking of market researchers to safeguard the rights of respondents must remain the same.

These issues are dealt with under the provisions of Rules 3 and 4 of the International Code. These Rules require that:

- A respondent’s personal data may be used only for the purposes for which they were collected and to which the respondent has agreed. Under no

circumstances may they be used for any non-research purpose.

- Such personal data must never be disclosed to anyone outside the research organisation(s) responsible for the project (other than for the limited and fully-safeguarded exceptions for necessary research purposes referred to below under Rule 4); and in any case only to authorised personnel who need such access for the purposes of research.
- While any data remain in personalised form strict security arrangements must be in place, and enforced, to prevent any unauthorised access to them.

Organisations carrying out marketing research must have the appropriate internal procedures and controls in place, and are advised to establish ISO 9001 or equivalent Standards, to ensure that legislative and other requirements are not contravened. Putting such controls in place is primarily the responsibility of those organisations. Individual researchers subscribing to the ICC/ESOMAR International Code must however always ensure that their own conduct fully conforms to the principles summarised above and embodied in the Code's Rules.

Rule 3 When asking respondents for their co-operation in a marketing research project they must be told: (1) the identity of the organisation or individual who is collecting the data (see also Rule 8) (2) the type(s) of person or organisation who will receive the results (3) the general purposes for which the results will be used.

Respondents must also be informed, where it is not already obvious, that their co-operation in the project is entirely voluntary.

Where requested by the respondent the latter must be told how their name came to be selected for interview. They must also be assured that any personal data they provide will be used for statistical research purposes only and will not result at any stage in any direct marketing approach being made to the individual respondent.

Researchers and those working on their behalf (eg interviewers) must not, in order to secure the co-operation of respondents or others, make statements or promises that they know or believe to be incorrect – for example about the likely length of the interview or about the possibilities of being re-interviewed on a later occasion.

In addition, any assurances given to respondents must be fully honoured.

Where it is possible that the researcher might wish to re-contact the respondent for a further interview at a later date (for example in the case of a longitudinal research project) permission for this must be obtained from the respondent not later than the end of the first interview except in the rare cases where there is some valid methodological reason to the contrary.

A respondent is entitled to withdraw from an interview or research project at any stage and to refuse to co-operate in it further. Any or all of the information collected from the respondent must be destroyed without unreasonable delay if the respondent so requests.

Where fieldwork is subcontracted the researcher must ensure in the contract with the interviewers that the latter understand and fully conform to the requirements of Rule 3.

Rule 4 Before collecting or otherwise processing any personal data researchers must ensure that, if required by law, they and/or their organisation are appropriately registered with the relevant national data protection authority.

Since data protection legislation applies only to “personal data” researchers should wherever possible plan to “de-personalise” such data as soon as possible after collection and the completion of any necessary quality control checks on the data. Where for technical or other reasons this is not practicable then any data must be securely stored in a way which prevents any unauthorised access for any purpose other than one needed to meet the objectives of the research project.

As long as it remains possible to link particular individuals to their responses there must be adequate security arrangements in force to ensure that any personal data is not accessible, accidentally or otherwise, by unauthorised individuals either inside or outside the researcher’s organisation. Authorisation for such access must be given only on a “need-to-know” basis and exclusively for research purposes. Such security precautions are necessary for all types of personal data, especial care being essential with the security of any data which might be regarded as particularly sensitive for any reason.

Where - for example in the case of panel or other longitudinal research studies - it is technically necessary to maintain files of research data in a

form where the identity of respondents is (at least potentially) identifiable the existence of such a research database must be registered with the national data protection registrar whenever required by law. Taking into account the requirements of Rule 3, researchers must ensure that:

- the respondents involved have been adequately informed about, and agreed to, the nature of the research and the form of data processing involved
- they understand that they can withdraw from the research at any stage before or after it has started
- they have agreed to the maintenance of the necessary data file
- they understand that they have the right at any stage of the research to know what personal data are held on them in the files, and that while these data are still held in personalised form they can ask for part or all of them to be corrected or destroyed, and that the researcher must conform to any such requests whenever it is reasonable to do so
- a security system is in place which at all times effectively prevents any unauthorised person from having access to any personal data provided by respondents, and that the data are used exclusively for the purposes of scientific marketing research.

In any case where personal data are to be transferred between countries the researcher must ensure that the level of data protection applied to the processing of personal data in the other countries involved is at least as high as that applying in the country where the data were originally collected. If there is any doubt about this the appropriate level of data protection to be applied must be specified in a written contract with the relevant parties in those other countries.

A researcher must not disclose personal data to any person or body outside the research organisation(s) responsible for the project without the explicit permission of the respondent for such disclosure in accordance with the requirements of Rule 4. In addition, one of the following two provisions must apply:

- the disclosure is exclusively for the purposes of research and not for any other purpose. (Where the disclosure of respondents' names/identities is to a third party such as a subcontractor this must be essential for a research purpose such as data collection or analysis or further interview - for example, for an independent fieldwork quality control check)
- where researchers co-operating in the same survey need to exchange

respondents' personal data in order to carry out different elements of the study - for example, in a combined quantitative and qualitative research study. In such a case respondents must be told in advance that a different research agency may be contacting them for this purpose, and have agreed to this.

In all such cases the researcher in overall charge of the project must ensure that all parties concerned agree to abide by the requirements of the ICC/ESOMAR International Code, as elaborated by these Notes, and by the requirements of relevant data protection legislation. If any parties have not already formally subscribed to the Code the researcher must secure their agreement, in writing, to do so. It should be noted that even these limited exceptions may not be permitted in certain countries. In such cases the researcher must always comply with the national requirements on data protection.

Rule 5 The researcher must explicitly agree with the client arrangements regarding the responsibilities for product safety and for dealing with any complaints or damage arising from faulty products or product misuse. Such responsibilities will normally rest with the client, but the researcher must ensure that products are correctly stored

and handled while in the researcher's charge and that respondents are given appropriate instructions for their use.

More generally, researchers should avoid interviewing at inappropriate or inconvenient times. They should also avoid the use of unnecessarily long interviews; and the asking of personal questions that may worry or annoy respondents, unless the information is essential to the purposes of the study and the reasons for needing it are explained to the respondent.

Rule 6 The definitions of "children" and "young people" vary by country. If not otherwise specified locally, researchers should assume that such references apply respectively to those "under 14 years" and between "14-17 years." This issue is addressed in detail in the ESOMAR Guideline on Interviewing Children and Young People.

Rule 7 The respondent must be told at the beginning of the interview that recording techniques are to be used unless this knowledge might bias the respondent's subsequent behaviour. In the latter category of cases, the respondent must be told about the recording at the end of the interview and be given the opportunity to see or hear the relevant section of the record

and, if he/she so wishes, to have this destroyed.

Researchers should note that tape and video recordings of interviews with respondents constitute personal data for the purposes of the EU Data Protection Directive. Researchers carrying out research within the EU must therefore process information collected by such means in the same way as they would any other personal data they collect (ie, fully in accordance with the provisions of the ICC/ESOMAR Code, as elaborated by these Notes).

A “public place” is one to which the public has free access and where an individual reasonably could expect to be observed and/or overheard by other people (e.g., in a shop or on the street). The more specific issues that arise with tape and video-recording of interviews are dealt with in the ESOMAR Guideline on this subject (N.B. The Guideline also deals with the situation where interviews are to be observed by a client).

Rule 8 The name and address/telephone number of the company normally must be given to the respondent at the time of interview. In the case of subcontracted fieldwork the respondent must be given the relevant

details of the agency responsible for subcontracting the work.

In the case of research using the Internet the respondent must be given an appropriate e-mail address at which to contact the researcher.

Whenever possible “Freephone” or similar facilities should be provided so that respondents can check the researcher’s bona fides without cost to themselves.

SECTION C: THE PROFESSIONAL RESPONSIBILITIES OF RESEARCHERS

Section C of the ICC/ESOMAR Code is not intended to restrict the rights of researchers to undertake any legitimate marketing research activity and to operate competitively in so doing. However, it is essential that in pursuing these objectives the general public’s confidence in the integrity of marketing research is not undermined in any way. Section C summarises the responsibilities of researchers to the public at large as well as to the marketing research profession.

Rule 13 Researchers must ensure that appropriate security systems are in place to ensure that at all stages of a marketing research project they comply fully with the provisions of the ICC/ESOMAR Code, as elaborated by

these Notes, insofar as these relate to the protection of personal data.

Rule 14 The kinds of technical information that should be made available on request include those listed in the Notes to Rule 25. The researcher must not, however, disclose information that is confidential to the client's business, nor need he disclose information relating to parts of the survey that were not published.

Rule 15 The kinds of "non-research activity" that must not be associated in any way with the carrying out of marketing research include:

- enquiries whose objectives are to obtain personal information about private individuals per se, whether for legal, political, supervisory (e.g., job performance), private or other purposes;
- the acquisition of information for use for credit-rating or similar purposes;
- the compilation, updating or enhancement of lists, registers or databases that are not for scientific research purposes (e.g., those that may be used for direct marketing);
- industrial, commercial or any other form of espionage;
- sales or promotional approaches to individual respondents;
- the collection of debts; and

- fund-raising.

Certain of these activities - in particular, the collection of information for databases for subsequent use in direct marketing and similar operations - are legitimate activities in their own right. Researchers (e.g., those working within a client company) may be involved with such activities either directly or indirectly. In such cases it is essential that a very clear distinction be made between such activities and marketing research. Any work that involves the collection and use of personal data for non-research purposes (such as those listed above) must not be carried out under the name of marketing research or of a marketing research organisation as such, or be incorporated into a marketing research survey. Personal data collected for marketing research purposes must never be used in connection with non-research activities such as direct marketing.

However, the use of marketing research data in connection with non-research databases is permissible where researchers have first ensured that such research information has been fully depersonalised (i.e., anonymised). A common way of achieving this is by "modelling" the research data before its fusion with any other data. This is permissible

only if there is no risk that any data in the database which is derived from marketing research could be linked to individual respondents or Data Subjects.

These issues are considered at greater length in the ESOMAR Guideline on Maintaining the Distinctions between Marketing Research and Direct Marketing.

There are no additional requirements which apply to customer satisfaction research in cases where no personal data are disclosed outside the research organisation(s) responsible for the project. Furthermore, if a survey sample or mailing list has been provided for the project by an outside company (eg client or other research organisation) it is also reasonable for the researcher to notify that company of any names and addresses which have been found during the course of the survey to be no longer operational (eg because a respondent has died or moved away from the address given). The situation is more complex in the case of a study which may involve other data about identified respondents (eg specific queries or comments) being disclosed outside the research organisation: these issues are addressed in more detail in a separate ESOMAR Guideline on Customer Satisfaction Studies.

SECTION D: THE MUTUAL RIGHTS AND RESPONSIBILITIES OF RESEARCHERS AND CLIENTS

Code Section D is not intended to regulate the details of business relationships between researchers and clients except insofar as involving principles of general interest and concern. Most such matters should be regulated by individual business contracts. It is clearly vital that such contracts be based on an adequate understanding and consideration of the issues involved: the ESOMAR Guidelines on “Selecting a Marketing Research Agency” and “Reaching Agreement on a Marketing Research Project” address these issues.

Rule 17 The ban on disclosing the identity of “other” clients does not apply when such disclosure has been previously agreed with those clients (e.g., in the case of certain jointly-sponsored “industry” surveys).

Rule 18 The researcher must ensure that, wherever the use of any subcontractor may result in personal data being disclosed to that subcontractor, the latter will fully comply with all relevant data protection and related requirements as summarised in the Notes on Rule 4 above.

Although it is usually known in advance what subcontractors will be used, occasions do arise during the course of a project where subcontractors need to be brought in, or changed, at very short notice. In such cases, rather than cause delays to the project in order to inform the client, it will usually be sensible and acceptable to let the client know as quickly as possible after the decision has been taken.

Rule 20 This Rule does not prevent the researcher from discussing relevant sections of the client's research brief with an actual or potential sub-contractor of that researcher when this is necessary for the purposes of the research project. In such a case the researcher is, of course, responsible for ensuring that the subcontractor fully conforms to this and other requirements of the Code.

Rule 21 Research proposals, research designs and questionnaires are, under the Berne Convention, the property of the researcher by whom they were originally designed provided that:

- the material can be shown to be an original creation;
- the originator has explicitly laid claim in the appropriate way (in written form) to the copyright and can if

required produce the necessary evidence of this; and

- the copyright has not been transferred to another party (e.g., a client) by agreement between the parties involved.

The extent of protection in practice may to some extent depend upon the nature of the material and the interpretation of the law in different countries. However, whether or not plagiarism in a particular case is shown to have actually broken the law, it may well be unethical, and any serious example would be regarded as prima facie one of unprofessional conduct.

Rule 22 The proposed period of time for which research records should be kept by the researcher will vary with the nature of the data (e.g., whether they are personal or non-personal), the nature of the project (e.g., ad hoc, panel, repetitive) and the possible requirements for follow-up research or further analysis.

The researcher should take suitable precautions to guard against any accidental loss of the information, whether stored physically or electronically, during the agreed storage period. Researchers must not retain personal data for longer than is necessary for the purposes of the specific study. With respect to the retention of personal

data, researchers must ensure compliance with all relevant data protection legislation and the requirements of the ICC/ESOMAR Code, especially Rule 4, as elaborated in these Notes.

In the case of non-personal data, the period of time for which records should be kept normally will be longer for the stored research data resulting from a survey (tabulations, discs, tapes, etc.) than for primary field records (the original completed questionnaires and similar basic records). The precise format in which records are stored is normally less important than the basic requirement that (unless previously agreed to the contrary and except to the extent that the reconstruction may result in the records becoming personalised) it should be possible to “reconstruct” all the information originally collected. The period of storage must be disclosed to, and agreed by, the client in advance.

In default of any agreement to the contrary, in the case of ad hoc surveys the normal period for which the primary field records should be retained is one year after completion of the fieldwork while the research data should be stored for possible further analysis for at least two years.

Rule 24 On request, the client – or his mutually acceptable representative – may observe a limited number of interviews for this purpose. When this occurs the researcher must first obtain the agreement of the respondent concerned. In addition, any such observer must previously have agreed to comply with the provisions of the ICC/ESOMAR Code, especially Rule 4, as elaborated by these Notes. This agreement must be obtained in writing in any case where the observer has not already done this.

The researcher is entitled to be recompensed for any delays and increased fieldwork costs that may result from such a request. The client must be informed if the observation of interviews may mean that the results of such interviews will need to be excluded from the overall survey analysis because they are no longer methodologically comparable.

In the case of multi-client studies, the researcher may require that any such observer is independent of any of the clients.

Where an independent check on the quality of fieldwork is to be carried out by a different research agency the latter must conform in all respects to the provisions of the ICC/ESOMAR

Code, as elaborated by these Notes. An agreement in writing to this effect must be obtained from that agency in any case where it has not already so agreed. If the third party agency has been instructed by the client, and not by the researcher, the researcher must ensure that the client enters into such an agreement with the third party agency. In particular, the anonymity of the original respondents must be fully safeguarded and their names and addresses may be used exclusively for the purposes of backchecks, not being disclosed to the client. Similar considerations apply where the client wishes to carry out checks on the quality of data preparation work.

Rule 25 The client is entitled to the following information about any marketing research project to which he has subscribed:

(1) Background

- for whom the study was conducted
- the purpose of the study
- names of subcontractors and consultants performing any substantial part of the work

(2) Sample

- a description of the intended and actual universe covered

- the size, nature and geographical distribution of the sample (both planned and achieved); and, where relevant, the extent to which any of the data collected were obtained from only part of the sample
- details of the sampling method and any weighting methods used
- when technically relevant, a statement of response rates and a discussion of any possible bias due to non-response

(3) Data collection

- a description of the method by which the information was collected
- a description of the field staff, briefing and field quality control methods used
- the method of recruiting respondents; and the general nature of any incentives offered to secure their cooperation
- when the fieldwork was carried out
- in the case of "desk research," a clear statement of the sources of the information and their likely reliability

(4) Presentation of results

- the relevant factual findings obtained
- bases of percentages (both weighted and unweighted)
- general indications of the probable statistical margins of error to be attached to the main findings, and of the levels of statistical significance of differences between key figures

- the questionnaire and other relevant documents and materials used (or, in the case of a shared project, that portion relating to the matter reported on). The report on a project normally should cover the above points or provide a reference to a readily available separate document containing the information.

Rule 27 It is clearly impossible for a researcher fully to control the ways in which research findings are interpreted or applied once these are in the public domain. However, researchers should use their best endeavours to prevent any misinterpretation or misuse of research findings, and (as far as is practicable) to correct any such misinterpretation or misuse once they become aware that this has happened.

The publication of research findings may sometimes prove to be misleading because certain of the technical aspects or limitations of the research have not been fully appreciated and/or because the public presentation, explanation and discussion of the findings (eg in the media) have not clearly spelt out all the relevant considerations. This can happen accidentally, or as a result of the pressures on media time and space, rather than for any more undesirable reason.

Researchers can reduce the danger of such problems arising by making sure (eg in their contract for a research project) that they are consulted in advance by the client about the form in which any research findings will be published. If following publication it becomes clear that serious misinterpretation of the research and its findings has occurred, leading to misleading discussion of the implications of the research, the researcher should endeavour to correct such misinterpretation by any available and appropriate means.

In a case where the client does not consult and agree in advance the form of publication with the researcher, the latter is entitled to:

- (i) refuse permission for his name to be used in connection with the published findings and
- (ii) publish the appropriate technical details of the project (as listed in the Notes to Rule 25).

Rule 29 It is recommended that researchers specify in their research proposals that they follow the requirements of ICC/ESOMAR Code and that they make a copy available to the client if the latter does not already have one.

SECTION E: IMPLEMENTATION

The addresses to which queries, or reports of possible Code infringements, should be sent are those on the inside front cover of the Code itself. Any such communications should be marked “For the attention of” :

The Professional Standards Committee, ESOMAR, Vondelstraat 172, 1054 GV Amsterdam, The Netherlands
The International Secretariat, ICC, 38 Cours Albert 1er, 75008 Paris, France

Possible infringements of the ICC/ESOMAR Code by members of ESOMAR will be investigated initially by the Society’s Professional Standards Committee, which has powers to warn or reprimand offenders. If after initial investigation the case appears to be one that might call for more severe sanctions, it will be referred to ESOMAR’s Disciplinary Committee. This Committee, under an independent Chairman, has the powers to suspend or expel members found guilty, after further investigation, of any serious contravention of the Code. When appropriate the relevant authorities also will be notified (e.g., the National Data Protection Authority in the case of an infringement of data protection legislation).

The detailed disciplinary procedures are set out in the ESOMAR publication entitled “ESOMAR Disciplinary Procedures”. For a research agency to be eligible to be listed in the ESOMAR Directory, its chief executive officer must have signed an undertaking that the company will conform in all respects to the requirements of the ICC/ESOMAR Code, as elaborated by these Notes. Any breach of this undertaking may lead to the withdrawal of the Directory listing.

REFERENCES

ESOMAR Guidelines:

- Maintaining the distinctions between marketing research and direct marketing
- Customer satisfaction studies
- Conducting marketing and opinion research using the Internet
- Interviewing children and young people
- Tape and video-recording of interviews and group discussions
- Mystery shopping studies
- How to commission research,
- The ESOMAR/WAPOR guide to opinion polls, incl. ESOMAR’s Code for the publication of public opinion polls
- EPhMRA/ESOMAR Guideline on pharmaceutical marketing research
- The arbitration service

ESOMAR WORLD RESEARCH CODES & GUIDELINES

ANNEXE TO NOTES ON THE ICC/ESOMAR INTERNATIONAL CODE OF MARKETING AND SOCIAL RESEARCH PRACTICE 2001 EUROPEAN UNION DATA PROTECTION REQUIREMENTS

INTRODUCTION

Rule 2 of the ICC/ESOMAR International Code of Marketing and Social Research Practice (“ICC/ESOMAR Code” or “Code”) requires compliance with any and all national and international legal requirements affecting marketing research. This Annexe summarises requirements within the European Union (“EU”) relating to the collection and handling of personal data.

The base measure discussed in this Annexe is EU Directive 96/46/EC “on the protection of individuals with regard to the processing of personal data and on the free movement of such data” (“EU Data Protection Directive” or “Directive”). As approved by the European Parliament and Council, the EU Data Protection Directive requires EU Member States to enact conforming laws, regulations and administrative provisions and to enforce such measures in the manner described in the Directive.

Researchers operating within the EU should familiarise themselves with the provisions of the EU Data Protection Directive. But that alone is not sufficient. They also should review, and must comply with, national data protection requirements in the various EU Member States, at least those in which they are operating. The reason is that such requirements are not entirely uniform:

and also that their interpretation may in certain cases depend on how they are applied in practice in the individual countries.

This Annexe is designed to familiarise researchers with the core data protection principles established by the EU Data Protection Directive. Country-specific data protection requirements are not identified in the discussion that follows.

When carrying out research within the EU Researchers will therefore need to ensure that they have set up and follow appropriate operating procedures which conform to the requirements of the Articles summarised below.

PURPOSES OF THE EU DATA PROTECTION DIRECTIVE

Article 1 of the EU Data Protection Directive requires Member States to “protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.” In pursuing that objective, the Directive instructs Member States that they should “neither restrict nor prohibit the free flow of personal data between Member States” in an unnecessary or inappropriate manner.

DEFINITIONS

Article 2 of the EU Data Protection Directive sets forth the following definitions, which also appear in most Member State data protection measures:

- Consent — the freely given and informed agreement by a person (i.e., the “data subject”) to the processing of his/her personal data. The data subject may withdraw his/her consent at any time and may attach any condition or limitation he/she believes to be appropriate.
- Controller — the individual or undertaking (e.g. the Researcher or research agency) that determines (alone or jointly with others) the purposes for which, and the manner in which, personal data are or will be processed.
- Personal Data — any information relating to an identified or identifiable natural person (i.e., a private individual as opposed to a corporate or other comparable entity). An identifiable person is someone who can be identified, directly or indirectly, in particular by reference to an identification number or the person’s physical, physiological, mental, economic, cultural or social characteristics.
- Personal Data Filing System — any set of personal data which is structured, either by reference to individuals or by reference to criteria relating to individuals,

in such a way that specific information relating to a particular individual is readily accessible. This includes both automated and manual records, whether they are centralised, decentralised or dispersed on a functional or geographical basis.

- Processing of Personal Data — includes, but is not limited to, their 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, whether by automated means or otherwise.

NATIONAL LAWS

Article 4 of the EU Data Protection Directive provides guidance to controllers in deciding which national law applies to any data processing activities for which they have responsibility. It generally instructs controllers to comply with the law of the Member State in which the controller is established (i.e. is located) and in which processing is carried out. When the controller is responsible for, and/or established in, several Member States he must ensure that he complies with the laws of all these Member States in which data processing is taking place. (These requirements

cover all aspects of data processing, as defined above, including the use of processing equipment except where the latter is used solely for the purpose of transferring data through the territory of the Community).

If the controller on a particular project has not been established in any country within the EU, the controller must designate a representative who is so established. Article 4 provides, however, that any such arrangement is “without prejudice to legal actions [that] could be initiated against the controller himself.”

DATA QUALITY

Article 6 establishes certain principles relating to “data quality.” These state that personal data must be:

- processed fairly and lawfully;
- collected for specific, explicit and legitimate purposes and not ‘further processed’ in a way incompatible with those purposes (NB: The Directive provides that the ‘further processing’ of data for historical, statistical or scientific purposes is not to be deemed to be incompatible with the initial purpose(s) provided appropriate safeguards have been provided by the particular Member State(s).);

- adequate, relevant and not excessive in relation to the purposes for which they are to be collected and/or are to be further processed;
- accurate and, when necessary, kept up to date, with every reasonable step being taken to ensure that data that are inaccurate or incomplete, having regard to the purpose(s) for which they were collected or for which they are being further processed, are erased or rectified; and
- kept in a form that permits data subjects to be identified for no longer than is necessary (NB: Member States are required to establish safeguards for personal data stored for longer periods for historical, statistical or scientific purposes).

OTHER LIMITS ON DATA PROCESSING

Article 7 establishes certain additional criteria for the processing of personal data. In most cases, personal data may be processed only if “the data subject has unambiguously given his consent.” There are certain exceptions to this requirement but in general they are unlikely to apply to most marketing research work. Without the data subject’s consent, personal data may be processed only if needed to:

- perform a contract to which the data subject is a party or take steps at

the request of the data subject prior to entering into a contract;

- comply with a legal obligation to which the data controller is subject;
- protect the vital interests of the data subject;
- perform a task carried out in the public interest or in the exercise of official authority vested in the controller or a third party to whom the data are to be or have been disclosed; or
- serve other legitimate purposes, 'except where such interests are overridden by the... fundamental rights and freedoms of the data subject'

The processing of personal data falling within the last two categories (i.e., the "public interest/official authority" and "other legitimate purposes" categories) must be stopped if the data subject informs the data controller of a "justified objection."

SPECIAL CATEGORIES OF DATA

Article 8 defines such data as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" The processing of such data is prohibited unless one or more of the exceptions specified in the Directive have been

met. The most important of these exceptions, in the case of marketing research, is the first - namely where "the data subject has given his explicit consent to the processing of such data" (except in a case where national law prohibits the giving of such consent).

The remaining exceptions are in most cases less relevant to most marketing research and cover situations where:

- the data subject has given his/her explicit consent, except where national law prohibits the giving of consent;
- the processing is required to satisfy the obligations of the data controller in the field of national employment law and national law imposes 'adequate safeguards';
- the processing is needed to protect the vital interests of the data subject or another person and the data subject is physically or legally incapable of giving consent;
- the processing will be carried out in a controlled and otherwise appropriate manner by a foundation, association or other non-profit body with a political, philosophical, religious or trade-union aim 'and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and the data are not

disclosed to a third party without the consent of the data subjects'; or

- the processing relates to data that have 'manifestly [been] made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.'

Article 8 establishes a special, although carefully defined and limited, exception for health-related information.

According to subsection 3 of Article 8, health-related data may be processed — even without the data subject's consent — when 'required for the purposes of preventative medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.'

In the case of scientific Marketing Research which conforms to the data protection requirements of the ICC/ESOMAR Code the handling of special categories of data need not in general pose special problems, but it is essential that Researchers ensure that all their procedures are fully in accordance with

the relevant Rules and legislation when dealing with such data.

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10 specifies that, when data are obtained directly from a data subject, the controller or the controller's representative must inform the data subject of:

- the identity of the controller and of the controller's representative, if any;
- the purpose(s) for which the data are being collected and will be processed; and
- any further information the data subject may need to guarantee fair processing of the data — such as the types of person or organisation that will receive the data, the voluntary nature (or otherwise) of the data subject's participation, and the data subject's right to access and correct data concerning him/her.

While Article 11 imposes broadly similar requirements when the data are not obtained directly from the data subject, such requirements do not apply in the case of "processing for statistical purposes or for the purposes of statistical or scientific research" and where "the provision of such information proves

impossible or would involve a disproportionate effort”.

OTHER DATA SUBJECT RIGHTS

Article 12 confers upon data subjects the right to obtain from the data controller “without constraint at reasonable intervals and without excessive delay and expense” the following:

- confirmation concerning whether the controller is holding or otherwise processing personal data relating to him/her;
- information on the purpose(s) of the processing, the categories of data concerned, and the recipients or categories of recipients;
- information ‘in an intelligible form’ concerning the data relating to him/her being processed and the source of such data; and
- information, in certain circumstances, concerning the ‘logic’ underlying any automated data processing (this requirement however applies primarily to activities other than statistical and scientific marketing research).

Article 12 also gives data subjects the right to require ‘as appropriate’ the ‘rectification, erasure or blocking of data’ whenever the processing of such data does not comply with the

provisions of the EU Data Protection Directive, ‘in particular because of the incomplete or inaccurate nature of the data.’ If data have been corrected or are subject to erasure or blocking, the controller must alert any third parties to whom the data have been disclosed of the action that was taken, unless such notification ‘proves impossible or involves a disproportionate effort.’

However, Article 13 allows certain exemptions to the requirements of Article 12. Importantly it specifies that Member States may dispense with those requirements in cases which are ‘subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual,’ where ‘there is clearly no risk of breaching the privacy of the data subject’, and when ‘data are processed solely for the purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.’

Article 14 confers upon data subjects the right to object, ‘on request and free of charge, to the processing of personal data relating to him/[her] [that] the controller anticipates being processed for the purposes of direct marketing.’

That includes the right to be informed in advance — that is, before personal data are disclosed for marketing purposes to a third party ‘for the first time.’

CONFIDENTIALITY AND SECURITY

Articles 16 and 17 impose confidentiality and security safeguards. Most fundamentally, data controllers are required to take appropriate steps, including steps of a technical and organisational nature, to protect personal data from accidental or unlawful destruction or accidental loss, alteration or disclosure. Controllers also must enter into a written agreement with any subcontractor who is to process data on the controller’s behalf, confirming the subcontractor’s agreement to process personal data in accordance with the controller’s instructions and to implement technical and organisational measures equivalent to those required of the controller.

NOTIFICATION OF NATIONAL DATA PROTECTION AUTHORITIES

Article 18 instructs Member States to require the controller or his representative, if any, to register with the data protection authority before collecting or otherwise processing personal data. Member States may, where they so decide, allow registration on a generic

basis with a general - non-project-specific -filing being made by the controller, especially for “categories of processing operations which are unlikely, taking into account of the data to be processed, to affect adversely the rights and freedoms of data subjects.”

Whenever advance notification of a project is required, this must, according to Article 19, include at least the following information:

- the name and address of the controller and of his/her personal representative, if any;
- the purpose(s) of the processing;
- a description of the category or categories of data subject and of the data or categories of data relating to them;
- the recipients or categories of recipients to whom the data might be disclosed;
- proposed transfers of data to third countries (i.e., countries other than those within the European Economic Area, which consists of the EU Member States plus Iceland, Liechtenstein and Norway); and
- a general description permitting a preliminary assessment to be made of the appropriateness of the measures that will be taken to ensure the security of data processing.

INTERNATIONAL TRANSFERS OF PERSONAL DATA

Article 25 generally prohibits the transfer of personal data to any country outside the European Economic Area unless such country “ensures an adequate level of protection.” Judgements concerning adequacy are supposed to take into account a variety of factors, including the nature of the data, the purpose and duration of the proposed processing operations, the country of data origin and destination, and the legal requirements and professional standards observed in the particular country. If adequate safeguards have not been implemented in the third country, a national data protection authority nonetheless may authorise the transfer if convinced that the contract pursuant to which the transfer is to be made requires the recipient to afford an adequate level of security.

Article 26 exempts from the foregoing the following transfers of personal data to non-European Economic Area countries:

- transfers to which the data subject has given his/her unambiguous consent (this would include knowledge of the country and entity to which their personal data might be transferred);

- transfers that are needed for the performance of a contract between the data subject and the controller or to implement a pre-contractual commitment made at the request of the data subject;
- transfers that are needed for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;
- transfers that are needed or are legally required on important public interest grounds or for the establishment, exercise or defence of legal claims;
- transfers that are needed to protect the vital interests of the data subject; and
- transfers that are made from a register established pursuant to laws and regulations as being open for consultation by members of the general public or by any person who can demonstrate a legitimate interest.

SECTOR-SPECIFIC CODES OF CONDUCT

Article 27 instructs the EU Commission and Member States to encourage the drawing up of codes of conduct “intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to [the EU Data Protection] Directive, taking account of the specific features of the

various sectors.” Provision has been made for the submission of such codes to the pertinent national data protection authorities and the Working Party created by Article 29 of the EU Data Protection Directive.

REMEDIES, LIABILITY AND SANCTIONS

Article 22 through 24 confer upon the individual EU Member States responsibility for adopting “suitable” measures, including specific sanctions, ensuring full implementation of the EU Data Protection Directive. According to Article 22, Member State enforcement measures must include, at a minimum, recognition of “the right of every person to a judicial remedy for any breach of the rights guaranteed... by the national law applicable to the [data] processing in question.” Member States also must ensure that anyone damaged by an act incompatible with applicable data protection guarantees may “receive compensation from the controller for the damage suffered.”

ICC/ESOMAR INTERNATIONAL CODE

The core requirements of the EU Data Protection Directive, insofar as they concern marketing research, have been reflected in the ICC/ESOMAR

Code since the Code was first formulated over 50 years ago. Those of the Directive’s requirements, summarised above, which affect the carrying out of marketing research are taken into account in the Notes to the ICC/ESOMAR International Code.

It is important to emphasise that once data have been de-personalised, so that they no longer can be linked to any natural person, they do not constitute “personal data” as defined in the EU Data Protection Directive. The right that data subjects otherwise would have to access and otherwise control or object to data processing expires at such time. The ICC/ESOMAR Code and accompanying Notes incorporate the same limitation, which is based on acknowledgement that the privacy interests of data subjects cannot be compromised by the disclosure of data that can be linked to any individual.

Any self-regulatory code implementing the EU Data Protection Directive and/or related national laws must be accompanied by appropriate disciplinary procedures and sanctions. These are referred to in Section E of the ICC/ESOMAR Code and the accompanying Notes on this. A full description of the procedures to be utilised and the sanctions that may be imposed in the

event of a violation of the ICC/ESOMAR Code, including the provisions dealing with the processing of personal data, is contained in a separate ESOMAR publication entitled “ESOMAR Disciplinary Procedures”.

NOTES

* **Page 2** Readers' attention is called to the fact that the German-language version of the International Code is prefaced by a Declaration prepared by the German national market research associations. This sets out certain additional requirements which must be followed in order to conform with German legislation when carrying out research in that country. Copies of this Declaration are available on request from the ESOMAR Secretariat.

ESOMAR
Vondelstraat 172
1054 GV Amsterdam
The Netherlands
Tel +31 20 664 2141
Fax +31 20 664 2922

ESOMAR is the world organisation for enabling better research into markets, consumers and societies.

With 4000 members in 100 countries, ESOMAR's aim is to promote the value of market and opinion research in illuminating real issues and bringing about effective decision-making.

To facilitate this ongoing dialogue, ESOMAR creates and manages a comprehensive programme of industry-specific and thematic conferences, publications and communications as well as actively advocating self-regulation and the worldwide code of practice.



www.esomar.org