ESOMAR PRACTICAL GUIDE ON COOKIES

JULY 2012

ESOMAR
WORLD RESEARCH

Copyright © ESOMAR 2012

TABLE OF CONTENTS

ESOMAR publishes Guidelines to assist researchers in applying the fundamental principles underlying the ICC/ESOMAR International Code on Market and Social Research to fast developing areas such as online, mobile and social media research.

ESOMAR also publishes a number of Guides – the Practical Guide on Cookies being the latest in the series - which are intended to help researchers decide when and how to use certain techniques. For instance ESOMAR published the Practical Guide to Cloud Computing in October 2011.

Consult these useful resources at:

http://www.esomar.org/knowledge-and-standards/research-resources.php

ESOMAR Practical Guide on Cookies

OBJECTIVES OF THIS GUIDE

This Practical Guide offers guidance to market, social and opinion researchers who use Cookies and similar technologies such as web beacons when conducting online activities on how to implement the European Union's (EU) new e–Privacy Directive (often referred to as the 'Cookie law') at company level. This Directive applies not only to research but also other activities such as any user-facing corporate website containing promotional materials or other B2B marketing techniques including email marketing that companies use to store or access information on a user's device.

The Guide should not be considered as a complete compliance solution, as it cannot advise individual companies about which specific method to gain users' consent for Cookies is the most appropriate as this differs according to how each country interprets the law.

Rather it attempts to sensitise researchers to the main issues to be addressed and in particular to help companies with auditing Cookies and similar technologies that they use. It should also be highlighted that digital fingerprinting falls within the scope of the Directive[1]. Finally, you should be aware that other European data protection legislation (e.g. EU data protection directive 95/46/EC) also applies if the Cookies that you use contain personal data.

INTRODUCTION

The European Commission has strengthened the privacy rights of internet users. All companies now need to comply with EU and national legislation based on the EU Directive 2002/58/EC including amendments made with EU Directive 2009/136/EC, the so-called e-Privacy Directive. The following guidance relates to Article 5(3) of the e-privacy directive, amended by EU Directive 2009/136/EC (hereafter the Directive') which impacts all website operators, including research companies:

Article 5 (3): "Member States shall ensure that storing of information, or the gaining of access to information already stored, in the technical equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC[2], inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communication network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."[3]

ESOMAR's Guideline for Online Research[4] provides guidance for market researchers in addressing legal, ethical and practical considerations in using new technologies when conducting online research.

This new Guide provides additional practical tips on how to understand Article 5 (3) of the Directive in particular rather than any of the other Articles.

---

[1] This is covered in more detail in this guide in the section "What you need to know" paragraph 6 and will be complemented by further ESOMAR guidance issued at a later date on digital fingerprinting, online identifiers and other more detailed issues.

[2] See Article 10 & 11 of EU Directive 95/46/EC with regards to "Information to be given to the data subject".

[3] European Directive 2009/136/EC

[4] ESOMAR Guideline For Online Research, revised 2011.

To date, all but four EU countries have fully implemented the Directive (July 2012). Each EU member state is implementing the Directive in its own way. For example, the UK Information Commissioner's Office has provided comprehensive and detailed guidance but this only applies to operations subject to UK law; The Netherlands implemented the Directive on 8 June 2012 requiring all those subject to the law to immediately introduce an opt-in for Cookies, whilst the authorities in at least France and Spain have recently issued or updated their guidance, tailored to their national interpretation of the law.

Finally, the Article 29 Working Party – which gathers together the data protection supervisory authorities from the 27 EU member states, the European Data Protection Supervisor and the European Commission - released their Working Paper 194[5] representing their point of view (note: not legally binding) on Cookie Consent Exemption based on Article 5(3) of Directive 2009/136/EC.

COOKIES & CO.: DEFINITION OF TERMS USED IN THIS PRACTICAL GUIDE

The following list of definitions applies for this Practical Guide for the market, social and opinion research sector noting that other definitions may be used elsewhere.

Cookie: The term "Cookie" is used as a synonym for Cookies and similar technologies (e.g. web beacons including clear gifs and tracking pixels; javascript and user agents such as browser settings which determine what is extracted from the browser such as language settings, service package, operating system) that store information or access information already stored on a user's equipment.

User's equipment: This refers to devices such as computers, tablets, smartphones or other devices on which information can be stored or already stored information is accessed via a telecommunication network.

To check compliance with the Directive, Cookies and similar technologies described in the ESOMAR Guideline for Online Research[6] must be differentiated and the following list includes additional definitions which are useful for this Practical Guide:

Session Cookies: This Cookie is linked to user actions on a website for the duration of one session (a 'session' is typically a non-consecutive visit of websites). This means that the Cookie is only stored as long as the user is surfing on the website and expires directly after the session ends.

Persistent Cookies: This Cookie is stored for longer than one browser session and allows tracking of user's preferences as well as statistical reports.

First party Cookies: This Cookie is set by the same domain as the website that the user is visiting (as displayed by the URL in the browser address bar).

Third party Cookies: This Cookie is set by a different domain than the website that the user is visiting.

Domain: This is a group of unique sites or web pages that begin with the same domain suffix address e.g. example.com. Usually a domain represents a site and can include multiple sub-domains e.g. homepage.example.com, service.example.com, etc.

Web analytics service: This is the collection and processing of data related to an internet service based on unique browsers, visitors, sessions, devices or content requests using a first or third party Cookie. Web analytics provide statistical service reports and do not disclose any personally identifiable information to third parties without consent.

Digital fingerprinting (also known as Digital DNA, device ID or machine ID): uses different metrics on the device of a user e.g. browser settings including browser version, language etc., operating system and whether plug-ins are active. The combination of these metrics provides detailed information about the user that could be treated as personally identifiable data. The Electronic Frontier Foundation (EFF) offers a tool - Panopticlick - that provides information on how unique you are based on your Digital Fingerprint[7].

[5] Article 29 Data Protection Working Party WP 194 Opinion 04/2012 on Cookie Consent Exemption
[6] ESOMAR Guideline For Online Research chapter 4.1.1
[7] http://panopticlick.eff.org

1. APPLICABLE LAW

The way that the Directive is implemented will differ according to how the country, where your company that is using Cookies is based, interprets the law. You should check with your national data protection authority and/or telecommunication supervisory authority for recommended phrases on obtaining valid consent for Cookies subject to the law of the country where your company is based. You should be prepared to answer any questions about which country's law you are applying should for instance, a regulator or client ask.

If you are reaching out to respondents by operating in their native language which is other than the language of the country where your company is based, it would be good practice to acknowledge that respondents expect the law of the country to apply where they, the respondents, are based. Regulators would also enact enforcement action in this way.

2. WHAT YOU NEED TO KNOW – SOME FAQs

Cookies are used in different services that research companies offer, such as web analytics, online questionnaires or panel management.

1. Do you need to comply with the Directive?

Absolutely, as the Directive had to be implemented into law in every EU country by 26 May, 2011 and as privacy is a fundamental right of EU citizens, all market research companies need to ensure that they are now fully complying with the Directive and the law in all EU countries where they do business. Doing nothing is not an option as you will become a priority for enforcement action by the data protection and/or telecommunication supervisory authority.

2. Are there exceptions within the Directive for setting and using Cookies?

The Directive makes an exception for Cookies that are set "for the sole purpose of carrying out the transmission of a communication over an electronic communication network, or as strictly necessary in order for the provider of an information society service explicitly requested by" the user.

Market research Cookies e.g. for the purpose of web analytics most likely do not fall under this exception as they are not strictly necessary, but the Article 29 Working Party expressed its opinion "that first party analytics cookies are not likely to create a privacy risk when they are strictly limited to first party aggregated statistical purposes and when they are used by websites that already provide clear information about these cookies in their privacy policy as well as adequate privacy safeguards. Such safeguards are expected to include a user friendly mechanism to opt-out from any data collection and comprehensive anonymisation mechanisms that are applied to other collected identifiable information such as IP addresses."[8]

3. Is there a difference made between session and persistent Cookies?

The Directive does not differentiate between session and persistent Cookies. You should ensure that you comply with this legislation for both forms of Cookies.

[8] Article 29 Data Protection Working Party WP 194 Opinion 04/2012 on Cookie Consent Exemption p. 10

4. Does this mean that you need to have prior consent for setting and reading from a Cookie on a user's technical equipment?

Due to the fact that the Directive is implemented into national law, it may be interpreted differently in the different EU member states. Generally speaking, the Directive requires consent of the data subject (user or subscriber). The EU Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (reference: 95/46/EC) also requires consent where the Cookie contains personal data.

You should decide whether you need the user to opt-in (by obtaining their explicit prior consent) before you can set and read from the Cookie.

It is important to know how you are using the information obtained through the Cookies when deciding on the required consent strategy.

In many cases, consent to collect market research data is obvious e.g. a research respondent 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 and have their answers deleted if they request.

Furthermore, a research panel respondent has given his/her explicit consent before participating in an online survey because they normally accept the panel terms and conditions at the time of registration with the panel. For this reason, since the panel is a requested service, the respondent does not need to answer a specific question to give separate consent for setting the Cookie to enable a survey.

One acceptable example would be to present to the panel member a simple, user-friendly statement at the time of registering for the panels e.g. "Yes, remember me". See Appendix C of this Guide, presenting a sample cookie policy, which should be read in conjunction with Appendix 2 of the ESOMAR Guideline for Online Research, which provides another example of a Cookie privacy policy but within the general privacy policy framework for an organisation. You will need to adapt your policy's language to your individual panel, etc.

5. What about web analytics?

In most cases, a user has not given consent for web analytics services prior to using a website. It is therefore essential to work with the website owner on whose behalf the web analytics service is conducted to agree on aligned privacy policy statements and a legally compliant consent solution.

It is recommended to offer an opt-in solution wherever possible, bearing in mind the intention of the law and the requirements of the ICC/ESOMAR International Code.

6. What impact does the Directive have on the use of digital fingerprinting?

The Directive requires that you have consent from the user before placing Cookies or similar technologies or by accessing stored information. According to this definition, digital fingerprinting techniques almost certainly fall within the scope of the Directive, so you should be aware of exactly what type of digital fingerprinting you use and take legal advice on how the Directive is enforced in those countries in which you operate, particularly if you use digital fingerprinting without consent.

Please note: If the device fingerprinting process that you use requires access (even once) to already stored information on the terminal equipment (e.g. browser setting, Mac address etc.) on the terminal equipment, the e-privacy directive is applicable. Therefore, in practice, consent for such digital fingerprinting should be obtained at the time when the individual consents to participate in a research project, so that you do not need to ask the user an additional question because it would be considered a requested service.

You should also ensure that the information about digital fingerprinting is clearly given in the privacy policy statement to comply with the Directive. Appendix 2 of the ESOMAR Guideline for Online Research provides a comprehensive example of a Cookie privacy policy including for digital fingerprinting.

However, information gathered or accessed for digital fingerprinting must be subject to strict purpose limitation; it should not be used for any other purpose than quality control. If another purpose is intended for the data, then the user should be informed and their additional consent for this specific purpose should be obtained, depending on the applicable local law.

As this is a fast evolving area and there are many different types of digital fingerprinting technology, ESOMAR intends to expand its advice on digital fingerprinting in further guidance to be issued later, ESOMAR will also issue further guidance on online identifiers such as IP address.

PRACTICAL GUIDE FOR COOKIE AUDIT

How to conduct a Cookie audit?

It is essential that you have a full picture of the Cookies used within your organisation. This ESOMAR Practical Guide will help you to run a Cookie audit within your own organisation.

Step 1: Inventory List

First of all, prepare an inventory list that includes all services using Cookies or similar technologies that store information on a user's equipment, hereafter referred to by the general term 'Cookies'. You need to review all the online services you are offering: This includes not only your research services such as web analytics, online questionnaires, panels, but also your general company website, marketing tools, etc.

Identify all the information you are storing with Cookies.[9] To collect this information you will need to work with any clients on whose websites you are setting Cookies and your IT team for your own websites which run the services.

Step 2: Exemptions and Purpose

Each Cookie must be checked against the following exceptions within the legislation which exempt Cookies from prior consent:

a. For the sole purpose of carrying out the transmission of a communication over an electronic communication network, or

b. If strictly necessary in order for the provider of an information society[10] service explicitly requested by the subscriber or user to provide the service.

Note that Cookies for the purpose of web analytics services are unlikely to fall under exemption 'b'.

Furthermore, you should check that the Cookies are necessary for the purpose you have identified, otherwise you should stop using them.

You need a clear sense of the purpose for setting and using a Cookie. This purpose needs to be included in the privacy policy in a clear and understandable manner so that the user is aware of it.

Step 3: Privacy Policy

A privacy policy is essential to explain the use, purpose and legal framework to the user. You should check that you (as data processor or data controller) and your clients (as data controller) have a privacy

[9] For an example of how to do this, please see the Cookie audit documents in Appendices A and B. Appendix A refers to web analytics; Appendix B refers to online surveys.

[10] Research conducted online can be regarded as a information society service, but there is no regulation in either the EU's e-commerce Directive or the EU's Directive 98/34/EC (EU law on information society services) that affects research relevant to this guidance.

policy in place that is easily accessible for the user and which gives clear, meaningful and understandable information about the data you are collecting and processing. This does not mean copy/paste the entire results of your Cookie audit modelled on appendices A/B of this Guide into your privacy policy. While the information in appendices A/B of this Guide is necessary to answer any questions from regulators and/or users, see the example privacy policy language given in Appendix C.

If you set third party Cookies on your client's website, ensure that you have a clear, written agreement with your client that the terms for setting and processing of Cookies are included in your client's overall privacy policy.

You should also ensure that you have a data processor contract in place if you are working on behalf of your client to collect information on their website.

Step 4: Consent Strategy

Review your strategies for obtaining consent from your online research participants and website users.

The consent strategy should be an opt-in wherever possible if you are collecting and processing personal data (e.g. panels, online questionnaires). See section 2 'What You Need to Know' above for a panel example.

Obtaining an opt-out consent through a user's browser settings may be sufficient in certain countries for web analytics.

Remember to check whether more detailed consent requirements exist with each relevant national regulatory authority.

Step 5: Conclusions and Next Steps

First of all, check that all the Cookies you are setting are necessary for your services. This means that you should stop using Cookies that are not necessary for the service you are providing for your organisation or to your clients.

Secondly, check if you have provided all relevant information in your privacy policies about the purpose of the Cookie and how the data are used. This is also relevant for you to check with your clients if you have a 'data processor contract' in place with them.

Finally, check if at least an opt-out is provided so that the user can withdraw their consent for the use of Cookies if they so wish.

APPENDIX A: EXAMPLE OF A COOKIE AUDIT FOR WEB ANALYTICS

Service	Service to provide web analytics (website statistics) for: www.esomar-example.com
Responsible person (Service, IT)	John Example (Service) Marie Test (IT)
Cookie name	Count ESOMAR Example
Cookie ID	Random selected number (alpha numeric code) e.g. AStfNlsTeAkWNh8.EAgjIzwnCCwMEVInHlKPDw__
Cookie domain	.counting4uservice.com
First or third party Cookie	Third party Cookie as website domain and Cookie domain are different
If third party Cookie, who is responsible for this	Counting4uservice Ltd. Test Street 1 London, UK Contact person: Terry Counting
Data processing contract	Between ESOMAR and Counting4uservice: ESOMAR is the data controller; Counting4uservice is the data processor.
Session or persistent Cookie	Persistent Cookie
Persistent Cookie expiry date	5 years after setting the Cookie
Purpose of Cookie	Cookie and referred data are used for website statistics of esomar-example.com website to obtain information including page impression, visit information that provides insights into the use of the website.
Is this explained in your clients or your privacy policy?	Privacy policy for esomar-example.com can be found under esomar-example.com/privacypolicy and provides information about the purpose of the Cookie, the legal information, contact information, third party data processor and an opt-out service.
Do you provide an opt-in or opt-Out solution?	Opt-out solution that is specified in the privacy policy and can be found under: esomar-example.com/privacypolicy/opt-out and is referring to counting4uservice.com/ESOMAR/opt-out/

APPENDIX B: EXAMPLE OF A COOKIE AUDIT FOR ONLINE SURVEYS

Service	Online Survey Tool to run questionnaires on: www.esomar-example.com
Responsible person (Service, IT)	Linda Survey (Service) Brian Cookie (IT)
Cookie name	Survey ESOMAR Example
Cookie ID	Random selected number (alpha numeric code) e.g. AStfNlsTeAkWNh8.EAgjlzwnCCwMEVInHlKPDw__
Cookie domain	.esomar-example.com
First or third party Cookie	First party Cookie as website domain and Cookie domain are the same
If third party Cookie, who is responsible for this	
Data processing contract	Not relevant as data are processed by esomar-example
Session or persistent Cookie	Session Cookie
Persistent Cookie expiry date	
Purpose of Cookie	Cookie is used to operate the survey during the session in which respondent is answering the questionnaire
Is this explained in your clients or your own company's privacy policy?	Privacy policy for esomar-example.com will be found under esomar-example.com/privacypolicy and provides information about the purpose of the Cookie and the information about data processing which takes place following the survey.
Do you provide an opt-in or opt-Out solution?	Opt-in solution as before starting the survey esomar-example provides all information about the purpose of the survey, the data processing, data publishing etc. and in addition actively requests an opt-in (agreement) by the respondent.

APPENDIX C: EXAMPLE COOKIE SECTION FOR A PRIVACY POLICY

"Cookies

Cookies allow a web server to transfer data to a computer for record keeping and other purposes. We use Cookies and other technologies to, among other things, better serve you with more tailored information and facilitate your ongoing access to and use of the Site during each browser session.

We use Cookies on this website for three purposes. One of the Cookies that we use is designed to remember you from page to page as you access our Site and to ensure that any information that you submit to us during each particular browsing session is remembered for the duration of that particular browsing session. This "session" Cookie will be automatically deleted when you close your browser session once you have finished using the Site.

When you select a language preference upon entering the Site, another Cookie remembers that setting. This Cookie remains on your computer after you close your browser so that you do not have to choose a language the next time you visit.

Finally, we use a Cookie for web analytics purposes, which enables [company name] to compile statistical reports about the usage of the Site based on anonymous aggregated data, for example, a report of the number of unique browser sessions that requested content from the Site during a particular period of time. This helps [company name] to understand how visitors use the site so that [company name] can optimize it.

If you do not want information collected through the use of Cookies, there is a simple procedure in most browsers that allows you to decline the use of Cookies. Some features of the Site may not work properly if you decline the use of Cookies. To learn more about Cookies, please visit http://www.allaboutCookies.org/. In addition, for more information about our website analytics products or to opt-out of these measurement services, **please click here**."

ACKNOWLEDGEMENTS

Project Team for ESOMAR Practical Guide on Cookies

- **Adam Phillips** - Committee Chair, Chair of ESOMAR Professional Standards and Legal Committees and Managing Director, Real Research
- **René Lamsfuß** – Vice-President, Market Governance & Data Strategy Europe, The Nielsen Company (Lead Author)
- **Alexander Singewald** – Legal Consultant to ESOMAR Legal Committee, Singewald Consultants Group, ESOMAR Legal Committee.
- **David Stark** – Vice President, Integrity, Compliance and Privacy Officer, GfK, and member of ESOMAR Professional Standards and Legal Committees

The Project Team developed this Practical Guide acting on the request of ESOMAR's Legal Committee which has reviewed the text. Find out more details about ESOMAR Legal Committee on ESOMAR website: http://www.esomar.org/government-affairs/legal-committee.php

CONTACTS

For further queries or feedback about this Practical Guide, contact: public.affairs@esomar.org
ESOMAR – World Association for Social, Opinion and Market Research
Eurocenter 2, 11th floor
Barbara Strozzilaan 384
1083 HN Amsterdam
The Netherlands
Tel: +31 20 664 2141
www.esomar.org