EU Privacy Regulations: Consent requirements in an on-line environment.

By Avv. Felix Hofer¹

1. The Privacy Regulations in force within the European Union are currently contained in two Directives: (a) the original Data Protection Directive (No. 95/46/EC of 24 October 1995⁵ “on the protection of individuals with regard to the processing of personal data and on the free movement of such data”), (b) the ePrivacy Directive, adopted a few years later (No. 2002/58/EC of 12 July 2002⁶) with the specific intent to regulate “the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)”. Both Directives provide for a strict opt-in system and therefore require that “… that personal data may be processed only if: (a) the data subject has unambiguously given his consent” (so Article 7 of Directive No. 46/1996) and set (b) that “… the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user” (so Article 5/3 of Directive No. 58/2002).

In 2009 Directive No. 2009/136/EC⁷ has amended the provisions of Article 5/3 mentioned above with the following wording: “Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal 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, 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 communications 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.” In short, the provisions previously in force has been significantly strengthened by affirming the need of data subject’s “informed prior consent” for placing any - not strictly functional – access mechanism on an end user’s technical equipment.

No doubt, that in a society where more and more business activities are performed on-line, such consent requirements pose significant practical and technical challenges. In order to avoid differing interpretations and with the intent to offer useful guidance to the national Privacy Commissioners of the countries members to the European Union, the Article 29 Working Party¹ has dedicated repeated efforts to the task of how consent should be obtained from data subjects in an on-line environment.
2. Already back in 2010 the Working Party explained – in its Opinion 2/2010 [WP 171] adopted on 22 June 2010 and focusing on online behavioral advertising – that the ePrivacy Directive, in its amended version, was clear about the fact that “.. an ad network provider who wishes to store or gain access to information stored in a user’s terminal equipment is allowed to do so if: i) it has provided the user with clear and comprehensive information…., inter alia, about the purposes of the processing and; ii) it has obtained the user’s consent to the storage of or access to information on his or her terminal equipment, after having provided the information requested under i)”, additionally clarifying that “i) consent must be obtained before the cookie is placed and/or information stored in the user’s terminal equipment is collected, which is usually referred to as prior consent and ii) informed consent can only be obtained if prior information about the sending and purposes of the cookie has been given to the user. In this context, it is important to take into account that for consent to be valid whatever the circumstances in which it is given, it must be freely given, specific and constitute an informed indication of the data subject’s wishes. Consent must be obtained before the personal data are collected, as a necessary measure to ensure that data subjects can fully appreciate that they are consenting and what they are consenting to. Furthermore, consent must be revocable.”

The Working Party then passed on to indicating how consent could be (legitimately) obtained in an on-line environment and to flagging some criteria to the attention of the advertising and marketing industry. With respect to browser settings is was felt that including the basic uses/purposes of third party cookies in a website’s general terms and conditions and/or privacy policy does not meet the requirement of ‘informed prior consent’. Neither is ‘consent by implication (i. e. by use)’ to be deemed as a viable solution. Technical means capable of “bypassing” users’ browser settings meant to block cookies are also not acceptable. Finally, browser settings with agreement to receive future cookies in bulk are definitely incompliant.

To the purpose of achieving a valid consent, browser settings must engage data subjects in an “affirmative action” resulting in a clear choice in favor of accepting cookies and must “convey clear, comprehensive and fully visible information” about cookies’ uses and purposes.

Therefore, generic warnings about the placement of cookies and their uses and purposes may not be considered as a suitable solution. The same goes for “opt-out” mechanisms and their ‘implied choices’: in the Working Party’s opinion, they are not apt to result in compliance with the consent requirement.

While admitting to be “conscious of the current practical problems related to obtaining consent, particularly if consent is necessary every time a cookie is read for the purposes of delivering targeted advertising” and to be ware about the fact that in the ePrivacy Directive’s wording “.. users’ acceptance of a cookie could be understood to be valid not only for the sending of the cookie but also for subsequent collection of data arising from such a cookie” (therefore covering also the “.. subsequent ‘readings’ of the cookie that take place every time the user visits a website partner of the ad network provider which initially placed the cookie”), the Working Party feels that such an interpretation could easily result in a “once-for-ever” acceptance practice, not exactly in line with the Directive’s intention. It therefore considers essential implementing safety measures, such as: limiting the scope of consent in time (e. g. no longer than one year, with a limited lifespan of cookies placed) and seeking for a renewal of consent after such period, offering additional information about the fact that consent will imply targeted advertising (with specific indications
about the networks performing such practice), alerting periodically that monitoring is in place and providing a user friendly and easy to activate mechanism for revoking consent previously given.

3. In the following year, the Working Party released another extensive document – Opinion no. 15 [WP 187] dated 11 July 2011 – on the topic, meant to clarify the exact meaning of some terms frequently used in EU Privacy Regulations. This opinion intends to meet a specific request for input submitted by the EU Commission in order to achieve a better and common understanding on expression such as "indication", "freely given", "specific", "unambiguous", "explicit", "informed". The Commission’s concern originated from the fact that “in the online environment - given the opacity of privacy policies - it is often more difficult for individuals to be aware of their rights and give informed consent.”

On the premise that in the current EU Privacy Regulations “consent is used ... both as a general” (even though not the exclusive one) “ground for lawfulness ..” [of the processing of an individual’s personal data] “and as a specific ground in some specific contexts”, the Working Party found that “Member States have taken their own approach and, in some cases, this has led to diversity. The concept of consent has not always been transposed word for word at national level.”

So, what are we to consider when confronted with the requirement of ‘informed, freely given, specific, explicit and unambiguous consent’?

In the conclusions of its Opinion, the Working Party summarizes the essential characteristics of such requirement and explains that “consent”:

- Is one (but not the only one) of the legal grounds for legitimate data processing,
- When sought, has to comply with the indications set by Directive no. 46 of 1999 (and with some additional aspects established in Directive no. 58 of 2002),
- When obtained, does not exempt the data controller from all the other compliance obligations set by the Directives (such as the proportionality principle and the adoption of technical measures suitable to grant safe processing),
- Must be obtained from individuals in their full legal capacity,
- Is always subject to data subject’s right of withdrawal,
- Must necessarily be achieved before the processing starts, and then additionally clarifies that consent may be considered as:
  - ‘Freely given’, only if obtained without any “risk of deception, intimidation or significant negative consequences for the data subject” eventually not agreeing to the processing,
  - ‘Specific’, when it relates to the exact purposes of the processing as exposed in the in-advance notice provided to data subjects (therefore no ‘blanket consent’ being allowed),
  - ‘Informed’, when extensive and adequate information has been provided to data subjects before the start of the processing, being implied that such information has to be offered not in “overly complicated legal or technical jargon”, but in in appropriate and easy to understand language as well as directly and in an easily accessible way (therefore ‘availability somewhere’ not meeting such requirement),
  - ‘Explicit’, if achieved through an “active response”, allowing no doubts about data subject’s ‘express wish’ to have its data processed for a certain – specified – purpose (where pre-ticked consent boxes would not result as a suitable mean),
- ‘Unambiguous’, only where there is a mechanism or action in place that show individual’s clear agreement to the processing (being obvious that ‘consent by implication’ is not deemed as acceptable).

In its final remarks the Working Party also stresses that in an on-line environment “explicit consent as a general rule for all types of processing” does not appear to result in an effective and adequate standard. On the contrary, “unambiguous consent” – especially if additionally clarified and defined, in the context of the upcoming revision of the current Privacy regulations - would not only encompass ‘explicit consent’, but would also offer data controllers broader flexibility in coming up with simple and user friendly technical solutions for collecting and substantiating individuals’ consent to the proposed processing.

4. Just one year later the Working Party felt appropriate dealing with some aspects related to the so-called Cookie Directive (i. e. Directive no. 2009/136/EC), amending parts of the ePrivacy Directive (No. 2002/58/EC). With the aim of offering providers guidance on when they may consider themselves as exempt from seeking and obtaining users’ consent for placing cookies or similar access mechanism on an individual’s terminal device, it issued Opinion no. 4 [WP 194] of June 7th, 2012.

According to the Opinion, the following may legitimately claim the benefit of consent exemption as provided by the criteria laid down in Directive no. 2009/136/EC:

- "User input cookies" (i. e. first party ‘session cookies’, expiring at the session’s end),
- "Authentication cookies" (identifying users once they have logged in; but if used for secondary purposes such as behavioral monitoring or advertising, exemption would not apply),
- "User centric security cookies" (also known as ‘flash cookies’, used for storing technical data needed to play back video or audio content; but no additional information must be collected),
- "Load balancing session cookies" (which allow to distribute web server requests over a pool of machines instead of just one),
- "User interface customization cookies" (simply meant to store a user’s preference – e. g. as to language or result display - regarding a service across web pages),
- "Social plug-in content sharing cookies" (usually allowing social networks users to share contents they like with their ‘friends’; but attention has to be paid in order to make sure that the exemption criteria are exactly met).

In the Working Party’s view, the following instead fall under the user consent requirement:

- "Social plug-in tracking cookies" (when not strictly necessary and functional, but used for tracking individuals, both members and non-members, with third party cookies for additional purposes such as behavioral advertising, analytics or market research),
- "Third party cookies" (when ‘operationally’ used for behavioral advertising purposes),
- "Cookies used for first party analytics" (i. e. for statistical audience measuring of websites, for detecting the preeminent search engine keywords or for tracking down navigation habits; even though for such systems the WP finds that in most cases “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”)

5. Earlier this year the Working Party specifically addressed privacy concerns and issues involved by the simply booming use of apps on smart devices. Opinion no. 2 [WP 202] of 27 February 2013 contains a section dedicated to consent requirements in such particular context.
Considering that “when installing an app, information is placed on an end user’s device” and that “many apps also access data stored on the device” (such as: contact details, addresses, images, other personal documents, etc.), it is quite clear that under the ePrivacy Directive such a practice needs to be covered by users’ consent. While such requirement may be sufficiently met by downloading and installing an app (after clicking an “install” button) for such initial purpose, collecting information from an end user’s device is clearly a different issue and needs the targeted individual’s informed, freely provided and unambiguous affirmative choice. Therefore a “Yes I accept option” will not result suitable for meeting specific consent requirements: all purposes and further uses of the collected information will have to made patent and behavioral monitoring and profiling practices will have to be laid open. Different types of data accessed and collected by an app cannot achieve proper consent by simply clicking on an “Install” button, as consent may not result in a general or generic authorization formula, but in some cases may involve “granular acceptance”\textsuperscript{vii}. In addition, app developers will be well advised by carefully considering that, even after having achieved users’ consent, they have no free license for excessive or disproportionate processing of the data collected through the app. They should also remind that all processing purposes – as explained in the in-advance notice – must be strictly maintained and that any significant changes to their business models will require a new notice and additional consent. Finally, they will have to bear in mind that business partners or third parties, capable of gaining access through data collected via an app, are hold to respect strictly the processing purposes revealed to app users.

6. Recently the Working Party, aware of “a range of practical implementations … developed by websites in order to obtain consent for the use of cookies or similar tracking technologies”, has felt necessary offering further guidance on issues relating to the achievement of proper consent for cookie placement on an end user’s device.

It has therefore delivered additional suggestions - in Opinion no. 2 [WP 208] dated 2 October 2013 – to website operators and providers of on-line services making use of cookies for various purposes, such as: enhanced functionalities, analytics, targeted advertising or product optimization. In the Working Party’s view, operators are free to use any suitable mean for achieving consent, as long as their practices are apt to inducing targeted individuals to validly agreeing on the processing of their personal information through the use of cookies or of similar technologies.

On such premise, the Working Party starts by individuating the most common means put in place in order to seek for users’ consent and finds that operators and providers tend to rely on the following systems:
- “an immediately visible notice that various types of cookies are being used by the website, providing information in a layered approach, typically providing a link, or series of links, where the user can find out more about types of cookies being used,
- an immediately visible notice that by using the website, the user agrees to cookies being set by the websites,
- information as to how the users can signify and later withdraw their wishes regarding cookies including information on the action required to express such a preference,
- a mechanism by which the user can choose to accept all or some or decline cookies,
- an option for the user to subsequently change a prior preference regarding cookies.”
With respect to such systems, the Working Party feels that, “although it is important to note that whilst each” [practice] “may be a useful component of a consent mechanism, the use of an individual practice in isolation is unlikely to be sufficient to provide valid consent as all elements of valid consent need to be present”. It therefore passes on to reminding the main elements of valid consent, consisting in “specific information, prior consent, indication of wishes expressed by user’s active behaviour and an ability to choose freely”, where:

- ‘Specific information’ has to consist in “clear, comprehensive and visible notice on the use of cookies, at the time and place where consent is sought”, e. g. the entry page of a webpage where a user’s browsing session starts and where “users must be able to access all necessary information about the different types or purposes of cookies being used by the website” or should at least find a link to a location with a detailed description of the cookies in use as well of the cookies’ purpose(s); such ‘necessary information’ would also have to include indications about aspects such as: placement of third party cookies or third party access to data collected via operator’s cookies, cookies’ expiry date and users’ choice on (complete or partial) acceptance or refusal of cookie placement.

- ‘A time requirement’ must be considered, which involves an obligation of providing a consent system not allowing to set a cookie on a user’s device before the latter has made an explicit choice in favor of such placement.

- ‘A clear acceptance’ requirement has to result in a mechanism through which an adequately informed user can express – by adopting an active behavior or a positive action – his/her express choice in favor of the placement of cookies and the collection of his/her personal information through them. Such mechanisms may typically “.. include splash screens, banners, modal dialog boxes, browser settings ..” and expressing a choice via an ‘active behavior or a positive action’ may consist in “.. clicking on a link, image or other content on the entry webpage ..”, provided the choice is based on clear and comprehensive information about cookies’ purposes and is expressed via a system (e. g. an “Accept” button), made available close to the location of such information. User’s choice therefore must always result expressed in ‘conjunction’ with comprehensive purpose information. User’s passive attitude and absence of active behavior will never be considered as correct fulfillment of the requirement.

- ‘Freely given consent’ means that users must find at their disposal – right on the entry page – a mechanism allowing a real and meaningful choice with respect to cookie use on their terminal devices and offering an option to accept (entirely or partially) or to decline such placement. Browsing a website without receiving cookies (or by receiving just some of them) should be a standard situation for users and ‘general access’ to a site should not result conditional on consent to cookie use; such condition may cover and limit only access to certain, specific content.

Finally, the Working Party reminds operators and providers that cookies not functional and necessary to delivering a certain service, but intended to offer additional benefits must always provide for a real acceptance choice. An identical obligation has to be fulfilled with respect to cookies primarily set for tracking purposes.
7. To conclude, website operators and providers of services of the Internet society will have to accept the fact that under EU privacy regulations consent by implication mechanisms (such as: “By entering, using, registering, browsing, ... you accept”) will be deemed as suitable for achieving valid consent only in very few cases, i.e. when accompanied by – detailed, clear and easily accessible - purpose information and by additional systems allowing to show user’s conscious, meaningful and positive choice in favor of a certain data or cookie use and purpose. Here lies the technical challenge to the industry and its capacity of developing consent achievement mechanisms viable in the day-by-day reality of an on-line environment.

(Reference date of this paper: November 2013)

---

Felix Hofer is a named and founding partner of the Italian law firm Studio Legale Hofer Lösch Torricelli, in Firenze (50132), via Giambologna 2/rosso; he may be reached through the following contact details: Phone +39.055.5535166, Fax +39.055.578230 – e-mail: fhofer@hltlaw.it (personal) or info@hltlaw.it (firm e-mail).

Directive no. 95/46/EC of 24 October 1995 may be found at:

Directive no. 2002/58/EC of 12 July 2002 may be found at:

Directive no. 2009/136/EC of 25 November 2009 may be found at:

The Working Party was set up under Article 29 of Directive 95/46/EC. It acts as an advisory body to the EU Commission and has the specific task of: (a) offering expert opinion from member state level on questions of data protection, (b) promoting harmonized application of the general principles of the Directives in all Member States through co-operation between data protection supervisory authorities, (c) advising on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy. Its tasks are detailed in Article 30 of Directive 95/46/EC. All EU Member States have a representative in this body and the national DPAs will always conform their activities to the indications issued by this Advisory Board.

According to the Directive cookie placement goes exempt from the requirement of informed consent only if the cookie: (a) is used for “the sole purpose of carrying out the transmission of a communication over an electronic communications network”, (b) “is strictly necessary for the provider of an information society service explicitly requested by the subscriber or user to provide the service”.

According to the Working Party “granular consent means that individuals can finely (specifically) control which personal data processing functions offered by the app they want to activate”, so Opinion no. 2/2013, page 15.