# The role of informed consent in privacy law

Zuiderveen-Borgesius, F.

**Publication date**
2015
**Document Version**
Final published version
**Published in**
Personal Data and Privacy

WIK-Consult • Report

Study for Ofcom

# Personal Data and Privacy

Final Report

Authors:
Dr René Arnold
Annette Hillebrand
Dr Martin Waldburger

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Germany

Bad Honnef, 26 May 2015

wik CONSULT

# 2 The role of informed consent in privacy law[12]

## 2.1 Fundamental rights and general data protection law

Consent plays a central role in most data privacy laws in the world.[13] With respect to online marketing practices, it is important to realise that in Europe informed consent is needed both for placing cookies or similar tracking devices on user's computers, according to the e-Privacy Directive, as well as for ensuing collection and processing of personal data, as regulated by the Data Protection Directive. There are instances in which consent is not required, e.g. if a cookie is necessary for transmission of communication, or for a service explicitly requested by the user. Furthermore, many personal data processing activities can be based on another legal basis than the data subject's consent. For instance, if the fulfilment of the specific service requires processing of personal data, consent is not always required. Nevertheless, consent plays a central role in the rules for online data processing.

The right to privacy is protected in various treaties.[14] In Europe, the right to privacy is included in Article 8 of the European Convention on Human Rights.[15] The European Court of Human Rights holds that the right to privacy protects people's Internet use against surreptitious monitoring: "the Court considers that the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8."[16]

In Europe, one of the main legal instruments to protect privacy and related interests in the context of digital data processing is data protection law. The right to protection of personal data is a fundamental right in the European Union, and is included in the 2000 Charter of Fundamental Rights of the European Union (legally binding since 2009). Article 8 of the Charter says: "Everyone has the right to the protection of personal data concerning him or her."[17] The second paragraph of Article 8 illustrates the important role of consent: "Such data must be processed fairly for specified purposes *and on the basis of the consent of the person concerned* or some other legitimate basis laid down by law" (emphasis added).

---

**12** This chapter has been written by Frederik Zuiderveen-Borgesius, Institute for Information Law (IViR), University of Amsterdam.

**13** For general principles on the principles of data privacy law in the world, see: Bygrave L. A. (2014): Data privacy law. An international perspective. Oxford University Press, chapter 5; Greenleaf, G. (2013): Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories. Journal of Law, Information & Science 23(1).

**14** See for instance Article 17 of the International Covenant on Civil and Political Rights; Article 12 of the UN Declaration of Human Rights.

**15** Article 8.

**16** ECtHR, Copland v. United Kingdom, No. 62617/00, 3 April 2007, par 44. Please note, this is a direct quote from the Court's Judgement and refers, with respect to the case of telephone, to information relating to the date and length of telephone conversations and in particular the numbers dialled.

**17** Article 8(2) of the Charter of Fundamental Rights of the European Union.

In daily practice, the national implementation law of the 1995 Data Protection Directive, such as the Data Protection Act 1998 in the UK, is most relevant. In the following text, we will concentrate on a description of the Data Protection Directive, which has laid the ground for national data protection laws in Europe, including that of the UK.

The Data Protection Directive only allows personal data processing if an organisation or company using personal data ("data controller"[18]) has a legal basis for the processing.[19] For companies processing personal data, the most relevant legal bases are Article 7(b), processing of personally data is a necessity for the performance of a contract between data controller and data subject, Article 7(f), according to which the processing must be necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject; and Article 7(a), i.e. the case that the data subject has given its unambiguous consent into the processing.[20]

For many personal data processing practices, no unambiguous consent is needed because one of the other legitimate reasons applies. For example, for a newspaper subscription, processing some personal data is necessary; the subscriber's address is necessary to deliver the newspaper. Hence, to process the subscriber's address, the newspaper company can rely on the legal basis of necessity for contract performance. The company does not have to ask the subscriber for separate consent for the use of the subscriber's address, as long as the company only uses that personal data to perform the contract.

For many innocuous standard business practices, a company can rely on the balancing provision. The balancing provision allows personal data processing, in short, if the company's interests outweigh the data subject's interests and privacy rights.[21] For example, a shop can send an existing customer paper brochures for the same type of products the customer bought before (i.e. first-party direct mail marketing).

If a company wants to process personal data, and cannot base the processing on the balancing provision or on another legal basis, only the data subject's "unambiguous consent" is required.[22] The Data Protection Directive defines consent as "any freely

18 The data controller is the "body which alone or jointly with others determines the purposes and means of the processing of personal data" (article 2(c) of the Data Protection Directive). The Directive distinguishes data processors (article 2(e)) from controllers. This report leaves that complication aside, and speaks of "company" for ease of reading.

19 Article 6(1)(b) of the Data Protection Directive requires a "legitimate purpose"; the literature usually speaks of a "legal basis". Article 7 lists the six possible legal bases for personal data processing.

20 The data subject is the person that personal data refer to (article 2(a) of the Data Protection Directive).

21 Article 7(f) reads as follows: "Member States shall provide that personal data may be processed only if: (…) (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)."

22 Article 7(a) of the Data Protection Directive.

given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[23] Consumers can always withdraw their consent.[24]

An indication of wishes can be given in many ways, and also implicitly. For instance, somebody can indicate his or her wishes by clicking an "I agree" button. However, an indication of wishes does require an expression of will.[25] Mere silence or inactivity of the data subject can generally not be interpreted as an expression of will.[26] This implies that opt-in systems are generally required for valid consent. With an opt-out system, where a data subject is presumed to "consent" if he or she does not object, there would almost never be an indication of wishes, as required by Article 2(h) of the Data Protection Directive ("unambiguous consent").

Furthermore, consent must be "informed" and "specific" to be valid. The controller must supply the data subject with the information s/he needs, such as the name and address of the controller, the processing purpose, the data recorded, etc.[27] The requirement that consent must be "specific" means that a consent request must concern "a particular data processing operation concerning the data subject carried out by a particular controller and for particular purposes".[28]

While consent plays an important role in data protection law, that role should not be exaggerated. First, as discussed in the above, for many personal data processing activities the law does not require prior consent, notably those covered by the other legitimate grounds in Article 7(b) and (f) of the Data Protection Directive (necessary for the performance of a contract or justified by a legitimate interest of the data controller that outweighs the data subject's interests). Second, even if a company has a legal basis for personal data processing, such as data subject consent or the balancing provision, the company must still comply with all the other requirements that follow from the Data Protection Directive.[29] In other words, even after the data subject has given his or her unambiguous consent for personal data processing, all the other data

---

**23** Article 2(h) of the Data Protection Directive.

**24** 1992 EC COM (92) 422 final amended proposal Data Protection Directive, p. 12.

**25** See: Article 29 Working Party, "Opinion 15/2011 on the definition of consent" (WP 187) 13 July 2011.

**26** Likewise, in general contract law, mere silence does not constitute an indication of will. See for instance Article 18(1) of the Vienna Sales Convention: "[a] statement made by or other conduct of the offeree indicating assent to an offer is an acceptance. Silence or inactivity does not in itself amount to acceptance."

**27** 1992 EC COM (92) 422 final amended proposal Data Protection Directive, p. 11. "To enable the data subject to make an assessment of the advantages and disadvantages of the processing of data concerning him, and to exercise his rights under Article l3 of the proposal (rectification, erasure and suppression), the consent given must be informed. The controller must supply the data subject with the information he needs, such as the name and address of the controller and of his representative if any (see Article 4(2)), the purpose of the processing, the data recorded, etc."

**28** 1992 EC COM (92) 422 final amended proposal Data Protection Directive, p. 12.

**29** See: Court of Justice of the European Union, Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González, not yet published, par. 71: "all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive (…)".

protection requirements still apply. For example, even after consent, companies may not process disproportionate amounts of personal data;[30] must secure the data they hold;[31] and may not use personal data for new purposes at will.[32]

***Informed consent in the Data Protection Directive***

- *Consent plays an important role in most data privacy laws in the world. The national implementation law of the 1995 Data Protection Directive is most relevant in the UK.*
- *Personal data processing requires a legal basis. For the private sector, consent, necessity for contract performance, and the balancing provision are the most important legal bases. Data subject consent is not required if personal data processing is a necessity for contract performance. Consent is also not required if processing is necessary for the legitimate interests of a company which processes personal data, and those interests are not overridden by the data subject's privacy rights.*
- *After the data subject's consent, data protection law as regards to e.g. the scope and period of data processing still applies in full.*

## 2.2 Informed consent in the e-Privacy Directive

Consent plays an especially important role in an online context. Article 5(3) of the 2009 e-Privacy Directive requires, in short, parties to obtain the user's consent before storing or accessing information on a user's device (subject to exceptions).[33] For the definition of consent, the e-Privacy Directive refers to the Data Protection Directive's consent definition: a freely given, informed and specific indication of wishes.[34]

Article 5(3) has several rationales. First, a user's devices, such as phones or computers, and the contents of those devices, are part of the user's private sphere as protected by the European Convention on Human Rights.[35] Therefore, such devices and their contents, such as saved messages, address books, etc., should not be read or accessed without the user's consent. Second, Article 5(3) protects users against placing spyware, tracking devices or other software on the devices without their

**30** Article 6(1)(c) and 6(1)(e) of the Data Protection Directive.
**31** Article 17 of the Data Protection Directive.
**32** Article 6(1)(b) of the Data Protection Directive.
**33** Article 5(3) of the e-Privacy Directive, amended in 2009.
**34** Article 2(f) of the e-Privacy Directive refers to the Data Protection Directive.
**35** Recital 24 of the e-Privacy Directive.

consent.[36] Third, Article 5(3) aims to protect people against surreptitious tracking of their activities.[37]

Article 5(3) also applies to storing and accessing cookies on people's devices. This application of Article 5(3) has received most attention in the recent debate. In brief, Article 5(3) requires consent for cookies, unless the cookie is necessary for transmission of communication, or for a service explicitly requested by the user. This implies, for instance, that no prior consent is required for using cookies for log-in procedures, for digital shopping carts or for language preferences.

The "indication of wishes" requirement has led to much discussion in the context of consent for cookies. While for instance the UK's ICO (Information Commissioner's Office) recommends opt-in boxes over other methods such as opt-out boxes, the ICO acknowledges with reference to the e-Privacy Directive that an opt-in box "is not necessarily the only way of obtaining consent".[38] This situation of ambiguity may have given support to claims that opt-out systems may be used to obtain "implied" consent. Some companies suggest people give consent to all types of cookies, including tracking cookies, if they have not changed the default settings on their browsers.[39]

The opt-in/opt-out discussion regarding cookies is likely caused by several factors. First, a recital of the 2009 Directive that amended the e-Privacy Directive says: "Where it is technically possible and effective, in accordance with the relevant provisions of [the general Data Protection Directive], the user's consent to processing may be expressed by using the appropriate settings of a browser or other application."[40] Some conclude that a user's default browser settings can express consent.[41] That interpretation has not been confirmed in case law. The interpretation seems hard to reconcile with the requirements of the Data Protection Directive, among other reasons because the recital

---

**36** Recital 24 of the e-Privacy Directive. "So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users."

**37** Recital 24 of the e-Privacy Directive: "hidden identifiers (…) can enter the user's terminal without their knowledge (…) to trace the activities of the user and may seriously intrude upon the privacy of these users." Recital 65 of Directive 2009/136: "Software that surreptitiously monitors the actions of the user or subverts the operation of the user's terminal equipment to the benefit of a third party (spyware) poses a serious threat to the privacy of users, as do viruses."

**38** Information Commissioner's Office (2013): Direct marketing. Data Protection Act. Privacy and Electronic Communications Regulations. Version 1.1, p 17-18.

**39** See e.g. Internet Advertising Bureau United Kingdom, "Department for Business, Innovation & Skills consultation on implementing the revised EU electronic communications framework, IAB UK Response" (1 December 2012) www.iabuk.net/sites/default/files/IABUKresponsetoBISconsultationonimplementingtherevisedEUElectronicCommunicationsFramework_7427_0.pdf, p 2.

**40** Recital 66 of Directive 2009/136.

**41** See e.g. Internet Advertising Bureau United Kingdom, "Department for Business, Innovation & Skills consultation on implementing the revised EU electronic communications framework, IAB UK Response" (1 December 2012) www.iabuk.net/sites/default/files/IABUKresponsetoBISconsultationonimplementingtherevisedEUElectronicCommunicationsFramework_7427_0.pdf, p 2.

refers to the Data Protection Directive, which requires an indication of wishes for consent.

Second, the scope of Article 5(3) has proven to be too broad in practice. For instance, Article 5(3) also requires consent for some website analytics cookies, as the provision does not contain an exception for such cookies. But it seems overly burdensome if website publishers must ask consent to use analytics cookies. And Internet users would likely not appreciate having to click "I agree" every time a website wants to use analytics cookies. The Article 29 Working Party, in which national data protection authorities cooperate, has suggested introducing an exception in the e-Privacy Directive for privacy-friendly analytics cookies, i.e. cookies that are strictly limited to the collection of first party anonymized and aggregated statistical purposes.[42]

Third, many websites allow third parties such as advertising networks to place tracking cookies, for instance for targeted marketing. Such websites might make less profit if they had to ask visitors for consent for placing such tracking cookies as visitors might not consent.

There are some variations in the way in which European Union member states have chosen to implement Article 5(3) at the national level. For instance, Ireland allows opt-out systems for obtaining consent for cookies, even though an active indication of wishes is lacking with such opt-out systems.[43]

***Informed consent in the e-Privacy Directive***

- *The e-Privacy Directive requires companies to obtain consent for placing or reading most types of cookies (and similar computer files) used for tracking purposes.*
- *There is an on-going discussion about how consent should be obtained.*

**42** Article 29 Working Party, „Opinion 04/2012 on Cookie Consent Exemption" (WP 194) 7 June 2012, p. 10-11.

**43** The Irish implementation of Article 5(3) says: "5. (1) A person shall not use an electronic communications network to store information, or to gain access to information stored in the terminal equipment of a subscriber or user, unless (…) (b) the subscriber or user is offered by the data controller the right to refuse to consent to that use." Irish Statutory Instrument (S.I. ) No. 535 of 2003 as amended by S.I. No. 526 of 2008 www.dataprotection.ie/viewdoc.asp?DocID=896 .

## 2.3 Future developments

Data protection law continues to evolve. In 2012, the European Commission published a proposal for a data protection regulation to replace the 1995 Data Protection Directive. Again, consent plays a central role in the proposal. The 2012 proposal always requires consent to be "explicit". That requirement has led to much lobbying; apparently, many companies prefer weaker requirements for consent.[44] The proposal is still being discussed in Brussels with negotiations probably ending in June 2015.[45] It is unclear, however, whether the proposal will be adopted in 2015.[46]

Technology also evolves. For instance, more objects are being connected to the Internet, leading to an "Internet of Things" (IoT). In IoT scenarios, the general Data Protection Directive and the e-Privacy Directive apply to many situations. The Data Protection Directive applies when "personal data" is processed; this is often the case in IoT settings.[47] For instance, if an Internet-connected refrigerator automatically orders groceries, some personal data such as the customer's delivery address must be processed to deliver groceries. The companies processing that data must comply with data protection law. If they want to use the personal data for more purposes than grocery delivery, they must, in many cases, obtain the data subject's consent.

Article 5(3) also requires companies to obtain the user's consent if companies access information on a user's device. The Article 29 Working Party gives the following example:

"A pedometer records the number of steps made by its user and stores this information in its internal memory. The user installed an application on his computer to download directly the number of steps from his device. If the device manufacturer wants to upload the data from the pedometers to its servers, he has to obtain the user's consent under Article 5(3) of directive 2002/58/EC [the e-Privacy Directive]."[48]

---

**44** For instance, Facebook proposes deleting the phrase "Silence or inactivity should therefore not constitute consent." (Facebook recommendations on the Internal Market and Consumer Affairs draft opinion on the European Commission's proposal for a General Data Protection Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data" https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/20121026_Drafting-recommendations_IMCO-draft-opinion_final.pdf).

**45** Lexology visited on 21-05-2015, see: http://www.lexology.com/library/detail.aspx?g=089098fa-41fd-461d-87dc-969584e8302d.

**46** See: Privacylaws.com, "Albrecht optimistic about 2015 deadline for EU DP Regulation" (23 January 2015) www.privacylaws.com/Int_enews_23_1_15.

**47** IoT devices often process both personal data and data that does not qualify as personal data.

**48** Article 29 Working Party, "Opinion 8/2014 on the Recent Developments on the Internet of Things" (WP 2234) 16 September 2014, p. 14.

***Future developments***

- *Informed consent plays a major role in data privacy law, and it will continue to play an important role in the future.*
- *The legal basis "consent" is often applicable in IoT situations.*