ARTICLE 29 DATA PROTECTION WORKING PARTY

01197/11/EN
WP187

Opinion 15/2011 on the definition of consent

Adopted on 13 July 2011

Executive Summary

The Opinion provides a thorough analysis of the concept of consent as currently used in the Data Protection Directive and in the e-Privacy Directive. Drawing on the experience of the members of the Article 29 Working Party, the Opinion provides numerous examples of valid and invalid consent, focusing on its key elements such as the meaning of "indication", "freely given", "specific", "unambiguous", "explicit", "informed" etc. The Opinion further clarifies some aspects related to the notion of consent. For example, the timing as to when consent must be obtained, how the right to object differs from consent, etc.

Consent is one of several legal grounds to process personal data. It has an important role, but this does not exclude the possibility, depending on the context, of other legal grounds perhaps being more appropriate from both the controller's and from the data subject's perspective. If it is correctly used, consent is a tool giving the data subject control over the processing of his data. If incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing.

This Opinion is partly issued in response to a request from the Commission in the context of the ongoing review of the Data Protection Directive. It therefore contains recommendations for consideration in the review. Those recommendations include:

(i) clarifying the meaning of "unambiguous" consent and explaining that only consent that is based on statements or actions to signify agreement constitutes valid consent;

(ii) requiring data controllers to put in place mechanisms to demonstrate consent (within a general accountability obligation);

(iii) adding an explicit requirement regarding the quality and accessibility of the information forming the basis for consent, and

(iv) a number of suggestions regarding minors and others lacking legal capacity.

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT OPINION

I. Introduction

The data subject's consent has always been a key notion in data protection, but it is not always clear where consent is needed, and what conditions have to be fulfilled for consent to be valid. This may lead to different approaches and divergent views of good practice in different Member States. This may weaken the position of data subjects. This problem has become more serious as the processing of personal data has become an increasingly prominent feature of modern society, both in on-line and off-line environments, often involving different Member States. This is why the Article 29 Working Party, as part of its Work Programme for 2010-2011, has decided to take a careful look into this subject.

Consent is also one of the subjects about which the Commission has asked for input in the context of the review of Directive 95/46/EC. The Commission Communication "A comprehensive approach on personal data protection in the European Union"[1] says that: *"The Commission will examine ways of clarifying and strengthening the rules on consent"*. The Communication explains[2] this as follows:

> *"When informed consent is required, the current rules provide that the individual's consent for processing his or her personal data should be a 'freely given specific and informed indication of his or her wishes by which the individual signifies his or her agreement to this data processing. However, these conditions are currently interpreted differently in Member States, ranging from a general requirement of written consent to the acceptance of implicit consent."*
>
> *"Moreover, 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. This is even more complicated by the fact that, in some cases, it is not even clear what would constitute freely given, specific and informed consent to data processing, such as in the case of behavioural advertising, where internet browser settings are considered by some, but not by others, to deliver the user's consent."*

---

1 COM (2010) 609 final of 4.11.2010.

2 The Commission's first report on the implementation of the Data Protection Directive (95/46/EC) (COM(2003)265 final, already mentioned on page 17: "The notion of "unambiguous consent" (Article 7(a)) in particular, as compared with the notion of "explicit consent" in Article 8, needs further clarification and more uniform interpretation. It is necessary that operators know what constitutes valid consent, in particular in on-line scenarios."

"Clarification concerning the conditions for the data subject's consent should therefore be provided, in order to always guarantee informed consent and ensure that the individual is fully aware that he or she is consenting, and to what data processing, in line with Article 8 of the EU Charter of Fundamental Rights. Clarity on key concepts can also favour the development of self-regulatory initiatives to develop practical solutions consistent with EU law."

To meet the Commission's request for input and to execute its Work Programme for 2010-2011, the Article 29 Working Party has committed to draft an Opinion. The goal of the Opinion is to clarify matters to ensure a common understanding of the existing legal framework. At the same time, this action follows the logic of earlier Opinions on other key provisions of the Directive[3]. Potential changes to the existing framework will take a while, so clarifying the current notion of "consent" and its main elements has its own virtues and advantages. Clarifying the existing provisions will also help to show which areas need improvement. Thus, building on the analysis, the Opinion will endeavour to formulate policy recommendations to assist the Commission and policy makers as they consider changes to the applicable data protection legal framework.

The basic content of the Opinion is as follows: After providing an overview of the legislative history and role of consent in data protection legislation, we examine the different elements and requirements for consent to be valid under applicable law, including some relevant parts of the e-Privacy Directive 2002/58/EC. The analysis is illustrated with practical examples based on national experiences. This exercise supports the recommendations, in the final part of this Opinion, that say that certain elements have to be in place to seek and obtain valid consent under the Directive. It also provides policy recommendations for policy makers to consider in the context of the review of Directive 95/46/EC.

II. General observations and policy issues

II.1. Brief history

While some national data protection/privacy laws adopted in the seventies foresaw consent as one of the legal grounds for processing personal data[4], this was not echoed in the Council of Europe's Convention 108[5]. There are no apparent reasons for consent not playing a bigger role in the Convention[6].

At EU level, reliance on consent as a criterion for legitimising personal data processing operations was foreseen from the very beginning of the legislative process that ended

[3] Such as Opinion 8/2010 on applicable law, adopted on 16.12.2010 (WP 179) and Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16.02.2010 (WP 169).

[4] See for example, Article 31 of the French Loi n 78-17 of 6 January 1978 "relative a l'informatique, aux fichiers et aux libertés".

[5] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (referred to as "Convention 108"). It entered into force on 1 October 1985.

[6] Convention 108 introduced the notions of "lawful processing" and "legitimate purpose" (Article 5), but unlike Directive 95/46/EC did not provide a list of criteria for legitimate data processing. The consent of a data subject only played a role in the context of mutual assistance (Article 15). However, the requirement of "consent" was later on mentioned repeatedly in various Recommendations of the Committee of Ministers.

with the adoption of Directive 95/46/EC. Article 12 of the Commission's proposal[7] in 1990 set out the properties that consent had to have to legitimise data processing operations: it had to be "*expressly given*" and "*specific*". Article 17, on sensitive data, required that consent be "*express and written*". The Commission's amended proposal[8] in 1992 introduced text close to the definition of "the data subject's consent" in today's Article 2(g), replacing the original Article 12. It stated that consent had to be "*freely given and specific*". The reference to "*expressly given*" was replaced by consent as "*an express indication of his (the data subject's) wishes*". The explanatory memorandum accompanying the 1992 amended proposal[9] stated that consent could be achieved either orally or in writing. As for sensitive data, the requirement for "*written*" consent remained. In 1992 the Commission's amended proposal re-structured the previous proposal, and introduced an Article 7 that deals with legal grounds for processing. Article 7(a) stated that processing could be carried out if "*the data subject has consented*"; the original list included, as today, five additional legal grounds (in addition to consent), that can be used to legitimize the data processing.

The Council Common Position[10] in 1995 introduced the final (today's) definition of consent. It was defined as "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*". The main change from the 1992 Commission position involved deleting the word "*express*" that had preceded the word "*indication*". At the same time, the word "unambiguous" was added to Article 7(a), so it reads as follows: "*if the data subject has given his consent unambiguously*". The requirement for written consent for sensitive data was replaced with "*explicit consent*".

Council's reasons[11] did not specifically explain those changes. Page 4 however states that *"... a number of amendments have ... been made to ... introduce a measure of flexibility which guarantees equivalent protection ... but does not lead to any lowering in the level of protection; they allow the general principles to be applied in an efficient and non-bureaucratic way in keeping with the wide variety of ways in which ... data are processed*."

The role of consent was explicitly recognised in the EU Charter of Fundamental Rights in dealing with the protection of personal data. Article 8(2) states that personal data can be processed "*on the basis of the consent of the person concerned or some other legitimate basis laid down by law*". Therefore, consent is recognised as an essential aspect of the fundamental right to the protection of personal data. At the same time, consent under the Charter is not the only legal ground enabling the processing of personal data; the Charter explicitly recognises that the law may lay down other legitimate grounds, as is the case with Directive 95/46/EC.

---

7 Proposal for a Directive concerning the protection of individuals in relation to the processing of personal data, COM (90), 314 final, SYN 287 and 288, Brussels, 13 September 1990.

8 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data an on the free movement of such data, COM (92) 422 FINAL- SYN 287, Brussels, 15 October 1992.

9 See page 11 of the amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data an on the free movement of such data, COM (92) 422 FINAL- SYN 287, Brussels, 15 October 1992.

10 Common Position of the Council on the proposal for a Parliament and Council Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data, (00/287) COD, adopted on 15/03/95.

11 See page 4 of the Common Position.

In sum, the legislative history, particularly in the EU, shows that consent has played an important role in conceptions of data protection and privacy. At the same time, it shows that consent has not been deemed as the only legal ground for legitimising data processing operations. The legislative history of Directive 95/46/EC shows relative consensus on the conditions of valid consent, namely: *freely given, specific and informed.* However, it also shows some uncertainty over the ways in which consent may be expressed - whether it has to be explicit, written, etc. This is further analyzed below.

II.2. Role of concept: ground for lawfulness

General/Specific ground:

Consent is used in the Directive both as a general ground for lawfulness (Article 7) and as a specific ground in some specific contexts (Article 8.2(a), Article 26.1(a)). Article 7 cites consent as the first of six different bases to legitimise the processing of personal data, while Article 8 provides for the possibility of using consent to legitimise the processing of special categories of (sensitive) data, that would otherwise be prohibited. In this last case the standard for obtaining consent is higher, as this consent must go beyond the general standard of consent by being "explicit".

Furthermore, the Directive allows for interaction with other legislation, as mentioned in Recital 23: "*Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws*". The way this system works in practice is complex: 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. As an illustration, consent as a general concept is not defined in French data protection legislation, but its meaning has been precisely and consistently explained in the jurisprudence of the data protection authority (CNIL), in relation to the definition contained in the Data Protection Directive. In the UK, it has been developed by common law in reference to the wording of the Directive. In addition, consent has sometimes been explicitly defined in specific sectors, for instance in the context of e-privacy, e-government or e-health. The notion developed in specific legislation will therefore interact with that developed in general data protection legislation.

Consent is also a notion used in other fields of law, particularly contract law. In this context, to ensure a contract is valid, other criteria than those mentioned in the Directive will be taken into account, such as age, undue influence, etc. There is no contradiction, but an overlap, between the scope of civil law and the scope of the Directive: the Directive does not address the general conditions of the validity of consent in a civil law context, but it does not exclude them. This means, for instance, that to assess the validity of a contract in the context of Article 7(b) of the Directive, civil law requirements will have to be taken into account. In addition to the application of the general conditions for the validity of consent under civil law, the consent required in Article 7(a) must also be interpreted taking into account Article 2(h) of the Directive.

This interaction with other legislation is not only visible at national but also at European level. A similar understanding of the elements of the Directive has been drawn from other contexts, as shown by a judgment of the Court of Justice in the field of labour law[12]: consent was required in the context of giving up a social right. The Court interpreted the notion of consent in the context of Directive 93/104 concerning certain aspects of the organisation of working time. It stated that 'worker's agreement' required consent by the worker (not by a union on the worker's behalf), and read "agreement" (…) to mean freely given informed consent. It also held that the worker signing an employment contract with a reference to a collective agreement authorising an extension of working time did not meet the requirements that consent be freely and expressly given, with full knowledge of all the facts. This interpretation of consent in a specific context is very close to the wording of Directive 95/46/EC.

Consent is not the only ground for lawfulness

The Directive clearly presents consent as a ground for lawfulness. However, some Member States see it as a preferred ground, sometimes close to a constitutional principle, linked to the status of data protection as a fundamental right. Other Member States may see it as one of six options, an operational requirement that is no more important than the other options. Clarifying the relation of consent with the other grounds of lawfulness - e.g. in relation to contracts, tasks of public interest or legitimate interests of the controller, and the right to object - will help to highlight the role of consent in specific cases.

The order in which the legal grounds are cited under Article 7 is relevant, but it does not mean that consent is always the most appropriate ground to legitimise the processing of personal data. Article 7 starts with consent, and goes on to list the other grounds, including contracts and legal obligations, moving gradually to the balance of interests. It should be noted that the five other grounds following consent require a “necessity” test, which strictly limits the context in which they can apply. This does not mean that the consent requirement leaves more margin of manoeuvre than the other grounds in Article 7.

Moreover, obtaining consent does not negate the controller's obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality. For instance, even if the processing of personal data is based on the consent of the user, this would not legitimise the collection of data which is excessive in relation to a particular purpose.

Nor does obtaining consent allow the circumvention of other provisions, such as Article 8(5). Only in very limited circumstances can consent legitimise data processing activities which would otherwise be prohibited, notably in relation to the processing of some sensitive data (Article 8) or to allow the use of personal data for further processing, whether or not this is compatible with the original purpose. As a principle, consent should not be seen as an exemption from the other data protection principles, but as a safeguard. It is primarily a ground for lawfulness, and it does not waive the application of other principles.

[12] Judgment of the Court (Grand Chamber) of 5 October 2004, Pfeiffer, Roith, Süß, Winter, Nestvogel, Zeller, Döbele in joined Cases C-397/01 to C-403/01.

The choice of the most appropriate legal ground is not always obvious, especially between Article 7(a) and 7(b). Under Article 7(b), the processing must be necessary to perform a contract, or in order to take steps at the request of the data subject prior to entering into a contract, and no more. A data controller using Article 7(b) as a legal ground in the context of the conclusion of a contract cannot extend it to justify the processing of data going beyond what is necessary: he will need to legitimise the extra processing with a specific consent to which the requirements of Article 7(a) will apply. This shows the need for granularity in contract terms. In practice, it means that it can be necessary to have consent as an additional condition for some part of the processing. Either the processing is necessary to perform a contract, or (free) consent must be obtained.

In some transactions a number of legal grounds could apply, at the same time. In other words, any data processing must at all times be in conformity with one or more legal grounds. This does not exclude the simultaneous use of several grounds, provided they are used in the right context. Some data collection and further processing may be necessary under the contract with the data subject – Article 7(b); other processing may be necessary as a result of a legal obligation – Article 7(c); the collection of additional information may require separate consent – Article 7(a); still other processing could also be legitimate under the balance of interests – Article 7(f).

Example: buying a car
The data controller may be entitled to process personal data according to different purposes and on the basis of different grounds:
- Data necessary to buy the car: Article 7(b),
- To process the car's papers: Article 7(c),
- For client management services (e.g. to have the car serviced in different affiliate companies within the EU): Article 7(f),
- To transfer the data to third parties for their own marketing activities: Article 7(a).

II.3. Related concepts

Control

The notion of consent is traditionally linked with the idea that the data subject should be in control of the use that is being made of his data. From a fundamental rights perspective, control exercised through consent is an important concept. At the same time, and from the same perspective, an individual's decision to accept a data processing operation should be subject to rigorous requirements, particularly taking into account that in doing so, an individual may be waiving a fundamental right.

Although consent plays a role in giving control to data subjects, it is not the only way to do this. The Directive provides other means of control, in particular the right to object, but this is a different instrument to be exercised at a different stage of the processing, i.e. after the processing has started and based on a different legal ground.

Consent is related to the concept of informational self-determination. The autonomy of the data subject is both a pre-condition and a consequence of consent: it gives the data subject influence over the processing of data. However, as explored in the next chapter, this principle has limits, and there are cases where the data subject is not in a position to take a real decision. The data controller may want to use the data subject's consent as a means of transferring his liability to the individual. For instance, by consenting to the publication of personal data on the Internet, or to a transfer to a dubious entity in a third country, he may suffer damage and the controller may argue that this is only what the data subject has agreed to. It is therefore important to recall that a fully valid consent does not relieve the data controller of his obligations, and it does not legitimise processing that would otherwise be unfair according to Article 6 of the Directive.

The notion of control is also linked to the fact that the data subject should be able to withdraw his consent. Withdrawal is not retroactive, but it should, as a principle, prevent any further processing of the individual's data by the controller. The way this works in practice will be explored further below (Chapter III).

Transparency

A second dimension of consent relates to information: transparency towards the data subject. Transparency is a condition of being in control and for rendering the consent valid. Transparency as such is not enough to legitimise the processing of personal data, but it is an essential condition in ensuring that consent is valid.

To be valid, consent must be informed. This implies that all the necessary information must be given at the moment the consent is requested, and that this should address the substantive aspects of the processing that the consent is intended to legitimise. This would normally cover the elements of information listed in Article 10 of the Directive, but will also depend on when, and the circumstances in which, consent is requested.

Regardless of whether or not consent is given, the transparency of data processing is also a condition of fairness, which has its own value also after the moment the initial information has been provided

Activity/timing: ways to signify consent

This third dimension relates to the way in which control is exercised: in which ways can consent be expressed and when should it be sought in order to ensure that it is real consent? These questions have a decisive impact on the way in which consent is exercised and interpreted.

Although the timing for seeking consent is not spelt out in the Directive, it is clearly implied from the language of the various provisions which indicate that, as a general rule, consent has to be given before the processing starts[13]. Obtaining consent before the processing of data starts is an essential condition to legitimise the processing of data. This point is further elaborated below in Chapter III.B regarding the e-Privacy Directive.

[13] As an illustration, the German version of the Directive (and the German Federal Data Protection Law) uses the notion "Einwilligung". This notion is defined in the German Civil code as "prior acceptance".

Consent, considered as an authorization by the individual to allow the processing of data pertaining to him/her, may be expressed in different ways: Article 2(h) refers to any "indication"; it must be unambiguous (Article 7a) and explicit regarding sensitive data (*ex* Article 8). However, it is essential to emphasize the fact that consent differs from the right to object provided for in Article 14. While in Article 7(a) the controller cannot process the data until he obtains the consent of the data subject, in Article 7(f) the controller can process the data, subject to conditions and safeguards, as long as the data subject has not objected. As stated in the Working Party's Working Paper 114: "*the importance of consent constituting a positive act excludes de facto any system whereby the data subject would have the right to oppose the transfer only after it has taken pla*ce"[14].

For these reasons, the right to object *ex* Article 14 of the Directive should not be confused with consent. The latter is a legal ground to process personal data ex Article 7(a), 8.2(a), 26.1 or as foreseen in various provisions of Directive 2002/58/EC.

II.4. Appropriate use of consent as a legal basis

There is a need to emphasise that consent is not always the primary or the most desirable means of legitimising the processing of personal data.

Consent is sometimes a weak basis for justifying the processing of personal data and it loses its value when it is stretched or curtailed to make it fit to situations that it was never intended to be used in. The use of consent "in the right context" is crucial. If it is used in circumstances where it is not appropriate, because the elements that constitute valid consent are unlikely to be present, this would lead to great vulnerability and, in practice, this would *weaken* the position of data subjects in practice.

This approach has already been supported by the Working Party and the EDPS in their contributions to the discussions on the new data protection framework. It has been stated in particular that *"it is not always clear what constitutes true, unambiguous consent. Some data controllers exploit this uncertainty by relying on methods not suitable to deliver true, unambiguous consent"*[15] in violation of the conditions of Article 6 of the Directive. In the same line, the WP29 has observed that *"complexity of data collection practices, business models, vendor relationships and technological applications in many cases outstrips the individual's ability or willingness to make decisions to control the use and sharing of information through active choice"*[16].

It is therefore important to clarify the limits of consent and to make sure that only consent that is construed in a way according to the law is deemed as such.[17]

---

14 WP114 - Working document of the Article 29 Working Party on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.

15 Opinion of the European Data Protection Supervisor of 14 January 2011 on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union".

16 "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", 1 December 2009, WP 168.

17 Opinion of the European Data Protection Supervisor of 14 January 2011, op.cit.

III. Analysis of provisions

In this analysis we will focus on Directive 95/46/EC in chapter III.A. Some relevant parts of the e-Privacy Directive 2002/58/EC will be analysed in chapter III.B. It should be noted that the Directives are not exclusive of each other. The general conditions for consent to be valid, as foreseen in Directive 95/46/EC, apply both in the off-line and in the on-line world. Directive 2002/58/EC specifies these conditions for some explicitly identified on-line services, always in the light of the general conditions of the Data Protection Directive.

III.A Directive 95/46/EC

The concept of "the data subject's consent" is defined in Article 2(h) and subsequently used in Articles 7, 8 and 26. The role of consent is also mentioned in recitals 30 and 45. These provisions and all relevant details will be discussed separately and in this chapter.

III.A.1. Article 2(h)

According to Article 2(h) 'the data subject's consent' shall mean *"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"*. This definition contains different key elements that will be discussed below.

"… any … indication of his wishes ... signifying …"

There is in principle no limits as to the form consent can take. However, for consent to be valid, in accordance with the Directive, it should be an indication. Even if it can be "any" form of indication, it should be clear what exactly can fall within the definition of an indication.

The form of the indication (i.e. the way in which the wish is signified) is not defined in the Directive. For flexibility reasons, "written" consent has been kept out of the final text. It should be stressed that the Directive includes "any" indication of a wish. This opens the possibility of a wide understanding of the scope of such an indication. The minimum expression of an indication could be any kind of signal, sufficiently clear to be capable of indicating a data subject's wishes, and to be understandable by the data controller. The words "indication" and "signifying" point in the direction of an action indeed being needed (as opposed to a situation where consent could be inferred from a lack of action).

Consent should include any indication of a wish, by which the data subject *signifies* his agreement: it could include a handwritten signature affixed at the bottom of a paper form, but also oral statements to signify agreement, or a behaviour from which consent can be reasonably concluded. Beyond the classical example of a signature, dropping a business card in a glass bowl could therefore fall within the definition. The same applies if an individual sends his name and address to an organisation in order to obtain information from it. In this case his action should be understood to constitute to the processing of such data insofar as it is necessary to process and respond to the request.

In its opinion on the use of location data with a view to providing value added services (WP115), the Working Party has assessed how individuals should be put in a position to consent to services that require their automatic location (e.g. the possibility of calling a specific number to obtain information on the weather conditions at one's location). In that case, it has been acknowledged that, provided users are given full information in advance about the processing of their location data, calling the relevant number would amount to consenting to being located.

Example: Bluetooth advertising boards
There is a developing advertising tool consisting of boards sending messages asking for the establishment of a Bluetooth connection to send ads to people passing nearby. The messages are sent to people that have activated their Bluetooth devices on their mobiles. The sole activation of the Bluetooth function does not constitute a valid consent (i.e. the Bluetooth function could be activated for other purposes). On the other hand, when someone is informed about the service and approaches a few centimetres from the board with his or her mobile, there is, normally speaking, an indication of a wish: this shows which people are really interested in getting the ads. Only those people should be considered as having consented, and only they should receive the messages on their phones.

It is questionable whether the absence of any behaviour - or perhaps better: passive behaviour - could also be interpreted as an indication in very specific circumstances (i.e. a totally unambiguous context). The notion of "indication" is wide, but it seems to imply a need for action. Other elements of the definition of consent, and the additional requirement in Article 7(a) for consent to be unambiguous, support this interpretation. The requirement that the data subject must 'signify' his consent seems to indicate that simple inaction is insufficient and that some sort of action is required to constitute consent, although different kinds of actions, to be assessed "in context", are possible.

In practice, in the absence of active behaviour of the data subject, it will be problematic for the data controller to verify whether silence was intended to mean acceptance or consent. For example, a data controller may have not have the certainty needed to assume consent in the following case: let us imagine a situation where upon sending a letter to customers informing them of an envisaged transfer of their data unless they object within 2 weeks, only 10% of the customers respond. In this example, it is contestable that the 90% that did not respond did indeed agree to the transfer. In such cases the data controller has no clear indication of the intention of data subjects. Besides, he will have no evidence and will therefore be unable to demonstrate that he obtained consent. In practice, the ambiguity of a passive response will make it difficult to fulfil the requirements of the Directive.

"… freely given …"

Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent. If the consequences of consenting undermine individuals' freedom of choice, consent would not be free. The Directive itself foresees in Article 8.2(a) that in some cases, to be determined by Member States, the prohibition of the

processing of special categories of personal data may not be lifted by the consent of the data subject.

An example of the above is provided by the case where the data subject is under the influence of the data controller, such as an employment relationship. In this example, although not necessarily always, the data subject can be in a situation of dependence on the data controller - due to the nature of the relationship or to special circumstances - and might fear that he could be treated differently if he does not consent to the data processing.

In several opinions, the Working Party has explored the limits of consent in situations where it cannot be freely given. This was notably the case in its opinions on electronic health records (WP131), on the processing of data in the employment context (WP48), and on processing of data by the World Anti-Doping Agency (WP162).

In WP131, the Working Party mentioned that *"free consent means a voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other. Any consent given under the threat of non-treatment or lower quality treatment in a medical situation cannot be considered as 'free' ... Where as a necessary and unavoidable consequence of the medical situation a health professional has to process personal data in an EHR system, it is misleading if he seeks to legitimise this processing through consent. Reliance on consent should be confined to cases where the individual data subject has a genuine free choice and is subsequently able to withdraw the consent without detriment."* [18]

If, once consent is withdrawn, the data processing continues based on another legal ground, doubts could be raised as to the original use of consent as the initial legal ground: if the processing could have taken place from the beginning using this other ground, presenting the individual with a situation where he is asked to consent to the processing could be considered as misleading or inherently unfair. It would be different if there were a change of circumstances, for example if a new legal basis were to appear in the course of the processing, such as a new law regulating the database concerned. If this new ground can validly apply to the data processing, the processing can go on. However, in practice such circumstances are not frequent. In principle, consent can be considered to be deficient if no effective withdrawal is permitted.

The Working Party has taken a consistent position on the interpretation of free consent in the context of employment[19]: *"where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for the worker to refuse it is not consent.… An area of difficulty is where the giving of consent is a condition of employment. The worker is in theory able to refuse consent but the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and is therefore not valid. The situation is even clearer cut*

[18] WP162 on WADA reaches the same conclusion: *"The sanctions and consequences attached to a possible refusal by participants to subject themselves to the obligations of the Code (for example providing whereabouts filings) prevent the Working Party from considering that the consent would be, in any way, given freely"*.

[19] WP48 on the processing of personal data in the employment context. WP114 - Working document of the Article 29 Working Party on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 - is also relevant here.

where, as is often the case, all employers impose the same or a similar condition of employment."

Example: pictures on intranet
Consent in the context of employment may be valid, as the following example shows: a company decides to set up an intranet which will feature employees' names and main roles. Each employee is asked whether they would like to have their pictures uploaded alongside each name. Individuals who want to have their picture uploaded are invited to send a picture to a given address. Upon receiving adequate information, the action of an individual to send a picture would be deemed to be consent. If the company has digital pictures of each employee, and asks each one for their consent to have them uploaded for the above purposes, each employee clicking a button to signify their consent would also be deemed to be giving valid consent. In either case, the choice of employees as to whether their picture appears on the intranet is being fully respected.

The context of employment requires specific discussion: The cultural and social aspects of the employment relationship play a role here, as does the way the data protection principles interact with other legislation. In the context of employment, personal data can be processed for various purposes:

- Data necessary for the exercise of its tasks by the employee: application of Article 7(b) - necessity for the contract
- To determine employees' entitlement to acquire stock options: it could either be on the basis of consent - Article 7(a), or considered as inherent to the administrative aspects of the contractual work relationship - Article 7(b)
- Processing the social security number for social security purposes: Article 7(c) - legal obligation, or possibly Article 8(b) - obligations in the field of employment law
- Processing of ethnic data: in some countries, this could also be an obligation due to employment law - Article 8(b), while in other countries it would be strictly forbidden.

Although there may be a strong presumption that consent is weak in such contexts, this does not completely exclude its use, provided there are sufficient guarantees that consent is really free.

While a situation of subordination is often the main reason preventing consent to be free, other contextual elements can influence the decision of the data subject. They can have for instance a financial dimension, or an emotional or a practical dimension. The fact that the collection of data is performed by a public authority can also have some influence on the data subject. It can however be difficult to draw the line between a simple incentive and something that has a real influence on the freedom of the data subject to exercise a choice. The examples below try to illustrate the different nature of the efforts or costs to the individuals that could influence their decision.

Example - Electronic health records

In many Member States there is a move to create an electronic summary of patients' health records. This will allow healthcare providers to access key information wherever the patient needs treatment.

- In the first scenario, the creation of the summary record is absolutely voluntary, and the patient will still receive treatment whether or not he or she has consented to the creation of a summary record. In this case consent for the creation of the summary record is freely given because the patient will suffer no disadvantage if consent is not given or is withheld.
- In the second scenario, there is a moderate financial incentive to choose the e-health record. Patients refusing the e-health record do not suffer disadvantage in the sense that the costs do not change for them. It could be considered here as well that they are free to consent or not to the new system.
- In the third scenario, patients refusing the e-health system have to pay a substantial extra cost compared to the previous tariff system and the processing of their file is considerably delayed. This signifies a clear disadvantage for those not consenting, with the purpose to bring all citizens within the e-health system in a scheduled deadline. Consent is therefore not sufficiently free. One should therefore also examine the existence of other legitimate grounds to process the personal data or examine the application of Article 8.3 of Directive 95/46/EC.

Example: body scanners

The use of body scanners is developing in some public spaces, in particular in airports to access the boarding area. Considering that passengers' data are being processed at the moment the scanning takes place[20], the processing must comply with one of the legal grounds under Article 7. Going through body scanners is sometimes presented as an option to passengers, implying that the processing could be justified by their consent. However the refusal to go through body scanners might create suspicions, or trigger additional controls, such as the undertaking of a body search. Many passengers will consent to being scanned because by doing so they will avoid potential problems or delays, while their first priority is to get on board of their flight on time. Such consent is not sufficiently free. As the processing must be proved to be necessary (for public security reasons), the legitimate basis should not be found in Article 7 (a) but in an act of the legislator – Article 7(c) or (e) – resulting in an obligation for passengers to cooperate. The basis for the body scanner screening should thus be the legislation: this legislation could still foresee a choice between scanning and pat-down, however this choice would only be offered to the individual in a complementary perspective, as part of additional measures.

The nature of the data controller can also be decisive with regard to the choice of legal ground to process personal data. This is especially the case for data controllers in the public sector, where the processing of data is normally linked to the performance of a

[20] See the letter of 11 February 2009 from the Chairman of the Article 29 Working Party to Mr. Daniel CALLEJA CRESPO, Director in DG TREN on body scanners, in reply to the Consultation of the Commission on "the impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection". Available at http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009-others_en.htm.

legal obligation as mentioned in Article 7(c) or the performance of a task carried out in the public interest as mentioned in 7(e). Accordingly, the use of consent of the individual concerned to legitimise the data processing is not the appropriate legal basis. This is particularly clear in the case of processing of personal data by public authorities vested with authoritative powers - such as law enforcement authorities acting within the remit of their tasks in the field of police and justice activities. Police authorities cannot rely on the individual's consent for measures which have not been provided for, or would otherwise not be allowed by law.

It should be acknowledged, nevertheless, that even though States may have a legal duty to process personal data, the individual does not always have a duty to collaborate. There may be cases where "added value services" are provided to data subjects, which they can decide to use or not. But in most of the cases the processing is actually mandatory. It is often not so easy to identify whether the processing of personal data by public authorities rightfully relies on the consent of the individual. The processing of personal data in the public sector therefore often involves hybrid schemes, which can lead to uncertainty and abuse if wrongly justified by consent.

While consent may in exceptional cases be a valid ground for States to process personal data, a careful check should be performed on a case-by-case basis to assess whether consent is indeed sufficiently free. As the following examples demonstrate, when a public authority is the data controller, the legal ground for legitimising the processing will be the compliance with a legal obligation *ex* Article 7(c), or the performance of a task of public interest *ex* Article 7(e), rather than consent.

Example: e-government
New ID cards with electronic functionalities embedded in a chip are being developed in Member States. It may not be compulsory to activate the electronic services of the card. But without activation, the user could be prevented from accessing certain administrative services, which would otherwise become very difficult to reach (transfer of some services on-line, reduction of office opening hours). Consent cannot be claimed to be the legitimate ground to justify the processing. In this case the law organising the development of e-services, together with all the appropriate safeguards, should be the relevant ground.

Example: PNR data
The question of whether the consent of passengers can be validly used to legitimise the transfer of booking details ("PNR data") by European airlines to the US authorities has been discussed. The Working Party considers that passengers' consent cannot be given freely as the airlines are obliged to send the data before the flight departure, and passengers therefore have no real choice if they wish to fly.[21] The legal basis here is not the consent of the passenger but, rather in accordance with Article 7(c), the obligations foreseen in the international agreement between the EU and the US on the processing and transfer of Passenger Name Record (PNR) data.

21 See Opinion 6/2002 of the Article 29 Working Party on transmission of passenger manifest information and other data from airlines to the United States.

Example: national census
During a national census, the population is asked to answer various questions about their personal and professional situation. Answering these questions is compulsory. In addition, the census also includes a question to which the answer is clearly indicated as optional, concerning the means of transport used by the individual. Although there is certainly no free consent for the main part of the census, there is a free choice to answer this last optional question. This should not disguise the fact, however, that the main purpose followed by the State in issuing this questionnaire is to obtain answers. Generally speaking, consent does not constitute a valid ground in this context.

"… specific …"

To be valid, consent must be specific. In other words, blanket consent without specifying the exact purpose of the processing is not acceptable.

To be specific, consent must be intelligible: it should refer clearly and precisely to the scope and the consequences of the data processing. It cannot apply to an open-ended set of processing activities. This means in other words that the context in which consent applies is limited.

Consent must be given in relation to the different aspects of the processing, clearly identified. It includes notably which data are processed and for which purposes. This understanding should be based on the reasonable expectations of the parties. "Specific consent" is therefore intrinsically linked to the fact that consent must be informed. There is a requirement of granularity of the consent with regard to the different elements that constitute the data processing: it can not be held to cover "all the legitimate purposes" followed by the data controller. Consent should refer to the processing that is reasonable and necessary in relation to the purpose.

It should be sufficient in principle for data controllers to obtain consent only once for different operations if they fall within the reasonable expectations of the data subject.

Recently the ECJ issued a preliminary ruling[22] regarding Article 12(2) of the ePrivacy Directive, concerning the need for renewed consent of subscribers who had already consented to have their personal data published in one directory, to have their personal data transferred to be published by other directory services. The Court held that where the subscriber has been correctly informed of the possibility that his personal data may be passed to a third-party undertaking and s/he has already consented to the publication of those data in such a directory, renewed consent is not needed from the subscriber for the transfer of those same data, *if it is guaranteed that the data in question will not be used for purposes other than those for which the data were collected with a view to their first publication (paragraph 65).*

[22] Judgment of the Court of 5 May 2011, Deutsche Telekom AG (Case C-543/09). This case started with the referral made by the German Federal Administrative Court regarding telecom directories and in particular the interpretation of Article 25(2) of the Universal Service Directive (2002/22/EC) and Article 12(2) of the ePrivacy Directive (2002/58/EC). It is clearly linked to the special role of directories in the Universal Service Directive.

Distinct consent may nevertheless be needed if the controller intends to process the data for different purposes. For instance, consent could be given to cover both information about new products to the individual on and specific promotion actions, as this could be considered as falling within the reasonable expectations of the data subject. But a separate and additional consent should be requested to allow for the sending of the individual's data to third parties. The need for granularity in the obtaining of consent should be assessed on a case-by-case basis, depending on the purpose(s) or the recipients of data.

It should be recalled that the processing could have several different legal grounds: some data could be processed because they are necessary in the framework of a contract with the data subject, such as for product fulfilment and service management, and specific consent may be needed for processing beyond what is necessary for the performance of the contract, for instance to assess the payment capacities (credit scoring) of the data subject.

The Working Party has clarified this aspect of consent in WP131 on electronic health records (EHR): "Specific" consent must relate to a well-defined, concrete situation in which the processing of medical data is envisaged. Therefore a "general agreement" of the data subject - e.g. to the collection of his medical data for an EHR and to any future transfers of these medical data to health professionals involved in treatment - would not constitute consent in the terms of Article 2(h) of the Directive.

The same reasoning is expressed in WP115 on the use of location data with a view to providing value added services: *"(the) definition explicitly rules out consent being given as part of accepting the general terms and conditions for the electronic communications service offered. ... Depending on the type of service offered, consent may relate to a specific operation or may constitute agreement to being located on an ongoing basis."*

In the Court decision mentioned above in Chapter II under the "Role of consent", even if the term "specific" is not explicitly used, the reasoning also insists on the need for consent to be specific by stating that "*it is not sufficient that the relevant worker's employment contract refers to a collective agreement which permits such an extension"***.**

Example: social networks
Access to social network services is often subject to agreeing to different kinds of processing of personal data.

The user may be required to consent to receiving behavioural advertising to register with a social network service, without further specification or alternative options. Considering the importance that some social networks have acquired, some categories of users (such as teenagers) will accept the receipt of behavioural advertising in order to avoid the risk of being partially excluded from social interactions. The user should be put in a position to give free and specific consent to receiving behavioural advertising, independently of his access to the social network service. A pop-up box could be used to offer the user such a possibility.

The social network service offers the possibility to use external applications. The user is, in practice, often prevented from using an application if he does not consent to the transmission of his data to the developer of the application for a variety of purposes, including behavioural advertising and reselling to third parties. Considering that the application can run without it being necessary that any data is transferred to the developer of the application, the WP encourages granularity while obtaining the consent of the user, i.e. obtaining separate consent from the user for the transmission of his data to the developer for these various purposes. Different mechanisms, such as pop-up boxes, could be used to offer the user the possibility to select the use of data to which he agrees (transfer to the developer; added value services; behavioural advertising; transfer to third parties; etc).

The specificity of consent also means that if the purposes for which data is processed by the controller change at some point in time, the user must be informed and put in a position to be able to consent to the new processing of data. The information provided must in particular address the consequences of a refusal of the proposed changes.

"… informed …"

The last element of the definition of consent - but not the last requirement, as we will see below - is its informed character.

Articles 10 and 11 of the Directive set out an obligation to provide information to data subjects. The obligation to inform is therefore distinct but in many cases is obviously linked to consent. While consent does not always follow the provision of information (another ground in Article 7 can be used), there must always be information before there can be consent.

This means in practice that *"consent by the data subject (must be) based upon an appreciation and understanding of the facts and implications of an action. The individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues, in particular those specified in Articles 10 and 11 of the Directive, such as the nature of the data processed, purposes of the processing, the recipients of possible transfers, and the rights of the data subject. This includes also an awareness of the consequences of not consenting to the processing in question"*[23].

Consent will in many cases be obtained at the moment of collection of personal data, when the processing starts. In this case, the information to be provided coincides with what is listed in Article 10 of the Directive. However consent can also be requested "downstream", when the purpose of the processing changes. In this case the information to be provided will have to focus on what is needed in the specific context, in relation to the purpose.

[23] WP131 - Working Document on the processing of personal data relating to health in electronic health records.

Informed consent is particularly decisive in the context of transfers of personal data to third countries: *"it requires that the data subject (is) properly informed of the particular risk that his/her data are to be transferred to a country lacking adequate protection"* [24].

Two sorts of requirements can be identified in order to ensure appropriate information:

- Quality of the information - The way the information is given (in plain text, without use of jargon, understandable, conspicuous) is crucial in assessing whether the consent is "informed". The way in which this information should be given depends on the context: a regular/average user should be able to understand it.

- Accessibility and visibility of information - information must be given directly to individuals. It is not enough for information to be "available" somewhere. The Court of Justice has insisted on this point in its 2004 judgment[25], referring to an employment contract including conditions which were not spelt out in the contract but referred to. The information must be clearly visible (type and size of fonts), prominent and comprehensive. Dialogue boxes can be used to give specific information at the time when consent is requested. As mentioned above in relation to "specific consent", on-line information tools are especially useful in relation to social network services, in order to provide sufficient granularity and clarity to privacy settings. Layered notices can also be a useful tool here, as they contribute to giving the right information in an easily accessible way.

As time goes by, doubts may arise as to whether consent that was originally based on valid, sufficient information remains valid. For a variety of reasons, people often change their views, because their initial choices were poorly made, or because of a change in circumstances, such as a child becoming more mature[26]. This is why, as a matter of good practice, data controllers should endeavor to review, after a certain time, an individual's choices, for example, by informing them of their current choice and offering the possibility to either confirm or withdraw[27]. The relevant period would of course depend on the context and the circumstances of the case.

Example: crime mapping
Some police forces are considering publishing maps, or releasing other data, showing where particular types of crime took place. Usually safeguards built into the process mean that no personal data about the victims of crime is published, because crime is only linked to relatively broad geographical regions. However, some police forces want to pin-point crime more exactly, where the victim of a crime consents to this. In such a case it becomes possible to link more precisely the data subject with the place where a crime has been committed. However, the victim is not specifically told that identifiable information about him/her will be published openly on the internet and how this information can be used. Consent is therefore not valid in this case because victims may not fully understand the extent to which information about them is being published.

[24] WP12 - Working Document Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive. See also WP114 - Working document of the Article 29 Working party on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995.

[25] See footnote 12 (Chapter II.2)

[26] Working document 1/2008 on the protection of children's personal data, WP 147, 18 February 2008.

[27] The Article 29 Working Party made similar recommendation in Article 29 Opinion 171 on online behavioural advertising, adopted on 22.06.2010.

The more complex data processing is, the more can be expected from the data controller. The more difficult it becomes for an average citizen to oversee and understand all the elements of the data processing, the larger the efforts should become for the data controller to demonstrate that consent was obtained based on specific, understandable information.

Consent, as defined in Article 2(h), should be read together with the further requirements mentioned later in the text of the Directive. Article 7 adds the word "unambiguous" to the elements of the definition, and Article 8 adds the word "explicit" when the processing relates to the processing of specific categories of data.

III.A.2. Article 7(a)

Pursuant to Article 7(a) of the Directive, the unambiguous consent of the data subject constitutes a legal basis to process personal data. Thus, to be valid, in addition to the criteria set forth under Art 2(h), consent must also be *unambiguous.*

For consent to be unambiguous, the procedure to seek and to give consent must leave *no doubt* as to the data subject's intention to deliver consent. In other words, the indication by which the data subject signifies his agreement must leave no room for ambiguity regarding his/her intent. If there is a reasonable doubt about the individual's intention, there is ambiguity.

As further described below, this requirement compels data controllers to create robust procedures for individuals to deliver their consent; namely either to seek clear express consent or to rely on certain types of procedures that deliver individuals' clear inferred consent. The data controller must also be sufficiently certain that the person giving consent is actually the data subject. This is particularly relevant where consent is given by telephone or online.

A related issue concerns the proof of consent. Data controllers relying on consent may want, or need, to demonstrate that consent has been obtained, for example in the context of a dispute with a data subject. Indeed, in some cases, they may be asked for such evidence in the context of enforcement actions. As a consequence, and as a matter of good practice, data controllers should create and retain evidence showing that the consent was indeed given, i.e. the consent should be verifiable.

Let us now analyze the following methods for providing consent and assess whether they deliver unambiguous consent.

Express statements to signify agreement, such as signed agreement or written statements of the desire to agree, are procedures or mechanisms well suited to deliver unambiguous consent. At the same time, in principle, they provide evidence to the data controller that consent had been obtained.

Example: consent to receive promotional information by regular mail
A hotel asks individuals to include their postal address on a paper form if they wish to receive promotional information by regular mail. If the individual, after providing the postal information, signs the form to signify his/her agreement, this will constitute

unambiguous consent. In this case, consent will be both express and in writing. This procedure provides the data controller with adequate proof of having obtained consent from all customers insofar as the data controller retains all the signed forms.

However, not all forms of consent that may seem to be explicit will deliver consent. This issue was discussed in the recent ECJ Case (Volker und Markus Schecke v Land Hessen), which referred to the publication of the names of beneficiaries of various EU funds[28] and of the amounts received by each beneficiary. The Advocate General analysed whether the conditions for unambiguous consent were met in a case where individuals had signed a statement saying: "I am aware that Article 44a of Regulation … No 1290/2005 requires publication of information on the beneficiaries of [funds from] the EAGF and the EAFRD and the amounts received per beneficiary." The Advocate General concluded: *"Acknowledging prior notice that publication of some kind will happen is not the same as giving 'unambiguous' consent to a particular kind of detailed publication. Nor can it properly be described as a 'freely given specific indication' of the applicants' wishes in accordance with the definition of the data subject's consent in Article 2(h)."* She therefore concluded that the applicants had not given their consent to the processing (i.e. the publication) of their personal data within the meaning of Article 7(a) of Directive 95/46/EC.[29]

Express consent may also be given in the on-line environment. As in the off-line world, there are very suitable means for delivering unambiguous consent, as illustrated in the following example.

Example: on-line consent to be enrolled in a loyalty program
A hotel web site includes a reservation form, enabling individuals to reserve rooms in advance electronically. The on-line form where individuals introduce the desired dates and payment related information also includes a visible box to be ticked by individuals who want their data to be used for the purposes of enrolling them in a loyalty program. Ticking the box after having received relevant information would constitute express, unambiguous consent as the action of ticking the box is clear enough to leave no doubt as to the individual's wish to be enrolled in the loyalty programme.

Express consent may also be given orally, through statements intended to signify agreement. Express oral consent would be given in the following situation.

Example: oral consent to receive promotional information
Whilst paying at a hotel's checkout lane, the clerk at the counter asks clients if they would like to provide their address so that the hotel can send them promotional information. Individuals that respond by providing their postal address, after having

[28] European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD).

[29] Opinion of Advocate General Sharpston delivered on 17 June 2010, Volker und Markus Schecke GbR, in Joined Cases C-92/09 and C-93/09. It should be noted that the ECJ ruled in its judgment of 9 November 2010 that the data processing was not based on consent: *"63. The European Union legislation in question, which merely provides that beneficiaries of aid are to be informed in advance that the data concerning them will be published, thus does not seek to base the personal data processing for which it provides on the consent of the beneficiaries concerned."*

heard the request from the clerk and the relevant information, would be giving express consent. The action of providing their address may constitute an unequivocal indication of the individual's wish. However the data controller may choose to put in place mechanisms to prove more reliably that consent had been given.

In some circumstances unambiguous consent may be *inferred* from certain actions, in particular this will be the case when the actions lead to an unmistakable conclusion that consent is given. However, this depends on relevant information about the data processing having been given, enabling the individual to make a decision (who is the data controller, what are the purposes of the processing, etc).

Example: consent to be photographed
Whilst checking in at a hotel's check-in lane, the clerk at the counter informs guests that a photo-shoot will take place at one of the hotels' cafeterias that afternoon. Selected images will be used for marketing material, particularly for paper based hotel brochures. If hotel guests would like to be pictured, they are invited to be in the cafeteria during the relevant hours. A different cafeteria is available for those who do not want to be photographed.

Hotel guests that - having been informed - decide to go to the cafeteria during the shooting hours may be deemed to have given their consent to be photographed. Their consent is inferred from their action of going to the cafeteria where the photo-shoot is taking place at the relevant time. Going to the cafeteria constitutes an indication of the individual's wishes, which in principle may be deemed unambiguous insofar as there is little doubt that the individual going to the cafeteria wanted to be photographed. However, the hotel might consider it prudent to have documentary evidence of the consent obtained, in case the validity of such consent is challenged in the near future.

As already stated, the same requirements including unambiguous consent apply both in the off-line and in the on-line world. However, the Working Party notes that the risk of ambiguous consent is likely to be greater in the on-line world, this calls for specific attention. The next example illustrates a case where consent inferred from certain action (participation in an on-line game) does not meet the requirements for valid consent.

Example: on-line game
An on-line game provider requires players to provide age, name and address for the purposes of participating in the on-line game (distribution of players among ages and addresses). The website features a notice, accessible through a link (although access to such notice is not necessary to participate in the game), which indicates that by using the website (and thus providing information) players are consenting to their data being processed to deliver them marketing information, by the on-line game provider and by third parties.

Accessing and participating in the game is not tantamount to giving unambiguous consent to the further processing of their personal information for purposes other than the participation in the game. Participation in the game does not imply the individuals' intent to consent to processing other than what is necessary to play. This type of behaviour does not constitute an unambiguous indication of the individual's wish to have his/her data used for marketing purposes.

Example: default privacy settings
The default settings of a social network, which users do not necessarily need to access to use it, enable the entire "friends of friends" category making all the personal information of each user viewable to all "friends of friends". Users who do not wish to have their information viewed by "friends of friends" are required to click a button. If they remain passive, or fail to engage in the action consisting in clicking a button, they are deemed by the controller to have consented to having their data viewable. However, it is very questionable whether *not* clicking on the button means that individuals at large are *consenting* to have their information viewable by all the friends of friends. Because of the uncertainty as to whether the lack of action is meant to signify consent, not clicking may not be considered unambiguous consent.

The above example illustrates a case where the individual remains passive (e.g. lack of action or "silence"). Unambiguous consent does not fit well with procedures to obtain consent based on inaction or silence from individuals: a party's silence or inaction has inherent ambiguity (the data subject might have meant to assent or might merely have meant not to perform the action). The following example further illustrates this.

There is ambiguity in the situation where individuals are deemed to have provided consent if they have not responded to a letter where they are informed that lack of responding means that they are consenting. In this type of situation, the individual behavior (or rather lack of it) raises serious doubts as to whether the individual meant to signify agreement. The fact that the individual did not undertake any positive action does not allow to be concluded that he gave his consent. Thus, it will not meet the requirement of unambiguous consent. Besides, as further illustrated below, it will also be very difficult for the data controller to provide evidence showing that the individual consented.

The Working Party has stated the unsuitability of consent based on individuals' silence in the context of sending direct marketing through emails. "*Implied consent to receive such mails is not compatible with the definition of consent of Directive 95/46/EC ..... Similarly, pre-ticked boxes, e.g., on websites are not compatible with the definition of the Directive either*"[30]. The following example confirms this view:

Example: invalid consent for further uses of customer data
An on-line book retailer sends an email to its loyalty program customers informing them that their data will be transferred to an advertising company, which plans to use it for marketing purposes. Users are given two weeks to respond to the email. They are informed that a lack of response will be deemed consent to the transfer. This type of mechanism, whereby consent is derived from a lack of reaction from individuals, does not deliver valid, unambiguous consent. It is not possible to ascertain without any doubt that individuals have agreed to the transfer from their lack of response.

It follows from the above that, as a consequence of the requirement for consent to be *unambiguous*, data controllers are *de facto* encouraged to have in place procedures and

[30] Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, adopted on 27 February 2004 (WP90).

mechanisms that leave no doubt that consent has been given, either on the basis of an express action carried out by the individual or by being clearly inferred from an action carried out by an individual.

As mentioned above, a matter of good practice data controllers should consider putting in place relevant measures and procedures to show that consent has been given. The more complicated the environment in which they operate, the more measures will be necessary to ensure that consent is verifiable. This information should be put at the disposal of the data protection authority upon request.

III.A.3. Article 8.2(a)

Article 8 of the Directive provides special protection to "*special categories of data*" which by their nature are considered to be very sensitive. The processing of such data is prohibited unless at least one of several specified exceptions applies. Article 8(2)(a) provides that the prohibition will not apply if the data subject has given his/her *explicit consent* to the processing.

In legal terms "explicit consent" is understood as having the same meaning as express consent. It encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing. Usually, explicit or express consent is given in writing with a hand-written signature. For example, explicit consent will be given when data subjects sign a consent form that clearly outlines why a data controller wishes to collect and further process personal data.

Although explicit consent is traditionally in writing, be it on paper or in electronic form, as illustrated before in chapter III.A.2, this is not necessary so it can also be given orally. This is confirmed by the fact that the requirement for consent suggested under Article 8 to be in writing was deleted in the final version of the Directive. However, as illustrated in the same chapter, oral consent may be difficult to prove and, therefore, in practice, data controllers are advised to resort to written consent for evidentiary reasons.

The requirement for explicit consent means that consent that is inferred will not normally meet the requirement of Art 8(2). In this regard, it is worth recalling the Article 29 Working Party opinion on electronic health records[31] stating that "*In contrast to the provisions of Article 7 of the Directive, consent in the case of sensitive personal data and therefore in an EHR must be **explicit**. Opt-out solutions will not meet the requirement of being 'explicit'.....*".

Example: medical data for research
A patient who is informed by a clinic that his medical file will be transferred to a researcher unless he objects (by calling a number), will not meet the requirement of explicit consent.

[31] WP131 - Working Document on the processing of personal data relating to health in electronic health records (EHR).

As stated above in chapter II.A.2, individuals may give explicit consent, orally and also in writing, by engaging in an affirmative action to express their desire to accept a form of data processing. In the on-line environment explicit consent may be given by using electronic or digital signatures. However, it can also be given through clickable buttons depending on the context, sending confirmatory emails, clicking on icons, etc[32]. The endorsement of procedures that entail an affirmative action by the individual is explicitly recognised by Recital 17 of the e-Privacy Directive which states that "*Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website*".

Consent does not have to be recordable to be valid. However, it is in the interest of the data controller to retain evidence. Obviously, the strength of the evidence provided by a specific mechanism may vary, providing more or less evidence of the consent. Consent that has been obtained through a clickable button with the identity of the individual supported with an email address only will have much less evidentiary value than a similar process that is supported, for example with recordable consent mechanisms[33]. The need for strong evidence will also depend on the type of data collected and the purpose followed: an electronic signature will not be needed to consent to receiving commercial offers, but may be necessary to consent to the processing of certain types of financial data on-line. Explicit consent given in an on-line environment will need to be recordable so that it is accessible to be used for subsequent reference.[34]

In the light of the above, on-line registration forms, to be completed by individuals with their identification information and their agreement to the data processing will be considered to meet the requirement for explicit consent, provided that all other requirements are fulfilled. For example, to open a personalised on-line medical file, patients may give their consent by providing their contact details and ticking a specific box to signify their agreement. The use of stronger authentication methods - for example, the use of digital signatures - will of course achieve the same outcome and constitute stronger evidence[35].

In certain cases, Member States may decide that a given data processing operation must be legitimised on the basis of consent and specify the type of consent. For example, to apply for a health card containing access to a medical history, Member States may decide that individuals that register on-line must sign with a particular digital signature. This option will ensure that the consent is express; it also gives the data controller more assurance that it will be able to prove individuals' consent.

---

32 This interpretation is in line with EU legislation, mainly on electronic commerce and on the broader use of digital signatures, which has required Member States to amend their legislation containing formal requirements for documents to be "in writing" and to be "handwritten" so that their electronic counterparts are equally accepted, if certain conditions are met.

33 In this regard, see for example Greek and German law regarding the requirements of providing consent by electronic means requiring consent to be recorded in a secure manner, the possibility to be accessed by the user or subscriber any time and to be revocable at any time (Article 5(3) of the Greek Law 3471/2006 on the protection of personal data in the electronic communications sector; Article 13(2) of the German Law on Teleservices, Article 94 of the German Law on Telecommunications, and Article 28 (3a) of the German Federal Data Protection Law).

34 It is outside the scope of this Opinion to analyse the technical conditions that must be fulfilled by electronic documents and digital signatures to be accorded equivalent evidentiary value as their hand-written counterparts. This is a matter that goes beyond data protection legislation and which has been regulated at EU level.

35 This is because the use of certain types of digital signatures (advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device) are automatically presumed to have the same legal value as evidence as written ones.

III.A.4. Article 26.1

Article 26.1(a) foresees the unambiguous consent of the data subject as an exception to the prohibition to transfer data to non-adequate third countries. The reflections made above regarding Article 7(a) apply here as well. This means that, in addition to the requirements for valid consent *ex* Article 2(g), consent must also be unambiguous.

The Article 29 Working Party has devoted much effort to providing guidance on the application of Article 25 and 26 of the Directive, including the exception of consent. In this context it is worth recalling the Working Party's document WP12[36] on the meaning of unambiguous consent: "*Because the consent must be unambiguous, any doubt about the fact that consent has been given would also render the exemption inapplicable. This is likely to mean that many situations where consent is implied (for example because an individual has been made aware of a transfer and has not objected) would not qualify for this exemption*".

In the light of the above, unambiguous consent is more likely to be obtained when individuals engage in an affirmative action to signify their agreement to the transfer, for example, by signing a consent form or engaging in other actions that unmistakably support the conclusion that consent has been given.

In WP 114[37] regarding the use of consent for data transfers, the Working Party stated that "*Consent is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or even structural transfers for the processing in question. In fact, particularly if the transfer forms an intrinsic part of the main processing (e.g. centralisation of a world database of human resources, which needs to be fed by continual and systematic data transfers to be operational), the data controllers could find themselves in insoluble situations if just one data subject subsequently decided to withdraw his consent. Strictly speaking, the data relating to a person who had withdrawn his consent could no longer be transferred; failing this, the transfer would continue to be partially based on the data subject's consent, but an alternative solution (a contract, BCR, etc.) would have to be found for data relating to subjects who had withdrawn their consent. Relying on consent may therefore prove to be a "false good solution", simple at first glance but in reality complex and cumbersome.*"

III.A.5. Consent given by individuals lacking full legal capacity

Under Directive 95/46/EC there are no particular rules on obtaining the consent of individuals lacking full legal capacity, including children. It is important that this reality is taken into account in the context of the review of the Data Protection Directive. In addition to the issues raised above, consent of these persons presents its own, specific problems.

---

[36] WP12 - Working Document Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection Directive, adopted on 24 July 1998.

[37] Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, adopted on 25.11.2005.

With regard to children, the conditions for delivering valid consent vary from Member State to Member State. The Article 29 Working Party, has on several occasions, reflected on the issue of children's consent and researched national practices[38].

Previous work shows that when children's consent is sought, legal requirements may require obtaining the consent of the child and the representative, or the sole consent of the child if he or she is already mature. The ages when one or the other rule applies vary. There are no harmonized procedures for verifying a child's age.

The lack of general rules on this leads to a fragmented approach and does not recognise the need for a specific protection of children in specific circumstances, because of their vulnerability, and because it causes legal uncertainty, particularly as far as the way children's consent is obtained.

The Working Party considers that this absence of harmonisation has consequences in terms of legal certainty. Harmonising the conditions for allowing incapable individuals to exercise their rights at EU level, especially with regard to the age threshold, would certainly bring additional guarantees. However, the Working Party is aware that this may well go beyond the scope of data protection as it touches more generally on civil law issues. The Working Party draws the attention of the Commission to the challenges raised in this area.

Furthermore, the Article 29 Working Party believes that the interests of children and other individuals lacking full legal capacity would be better protected if the Directive contained additional provisions, specifically addressed to the collection and further processing of their data. These provisions could foresee the circumstances in which the consent of the representative is required, together with, or in place of, the consent of the incapable individual, and could foresee circumstances where it should not be possible to use consent as basis for legitimising the processing of personal data. It should also foresee the requirement to use on-line age verification mechanisms. There are different mechanisms and different thresholds. For example, age verification, rather than being subject to one single rule, could be based on a sliding scale approach whereby the mechanism to be used would depend on the circumstances, such as the type of processing (the purposes), whether particularly risky, type of data collected, data usages, (whether the data is intended for disclosure), etc.

III.B. Directive 2002/58/EC

The recently amended e-Privacy Directive (Directive 2002/58/EC)[39] is a *lex specialis* vis-à-vis Directive 95/46/EC insofar as it offers a sector specific regime with regard to privacy and electronic communications. Most of its provisions apply to providers of

[38] WP147 - Working Document 1/2008 on the protection of children's personal Data (General guidelines and the special case of schools); WP160 Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools).

[39] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, 18.12.2009.

publicly available electronic communication services only (e.g. providers of telephony, Internet service providers, etc).

Some of the provisions of the e-Privacy Directive rely on consent as the legal basis upon which providers of publicly available electronic communication services may rely in order to process data[40]. This is the case, for example, regarding the use of traffic or location data.

The Article 29 Working Party considers it useful to comment on selected aspects related to the use of consent under the e-Privacy Directive that are of particular interest. To this end, we will address the following five issues:

a) The relationship between the definition and overall meaning of consent between the Directive 95/46/EC and the e-Privacy Directive. This is based on Article 2.2(f) of the e-Privacy Directive.

b) The question of whether, to breach the confidentiality of communications (for example, to monitor or intercept a telephone communication), it is necessary to obtain the consent of one or both communicating parties. This is governed by Articles 6(3), and 5.1.

c) The question regarding the timing as to when consent must be obtained. This is addressed in various provisions of the e-Privacy Directive, including Article 5(3), 6 and 13.

d) The scope of application of the right to object and its distinction from consent. This distinction can be analysed under Article 13 of the e-Privacy Directive.

e) The possibility to withdraw consent as explicitly foreseen in Article 6.3 and 9.3-4 of the e-Privacy Directive.

III.B.1. Article 2(f) - Consent and relation with Directive 95/46/EC

"*consent of user or subscriber*"

Article 2 of the e-Privacy Directive explicitly states that the definitions of Directive 95/46/EC shall apply regarding Directive 2002/58/EC. Article 2(f) says "*consent by a user or a subscriber corresponds to the data subject's consent in Directive 95/46/EC*".

This means that whenever consent is required under the e-Privacy Directive, the criteria to determine whether consent is valid are the same as those set forth by Directive 95/46/EC, namely the definition in Article 2(g) and the specificity included in Article 7(a). The view that consent in the e-Privacy Directive must be understood by reference to Article 2(g) and Article 7(a) together is confirmed in Recital 17[41],

---

40 Traffic data means data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication, including data relating to the routing, duration or time of a communication.

41 It reads which says: "*For the purposes of this Directive, consent…should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC*"

III.B.2. Article 5.1. - Whether consent is necessary from one or two parties

"*… consent of users concerned …*"

Article 5(1) of the e-Privacy Directive protects confidentiality of communications by prohibiting any kind of interception or surveillance of communications without the consent of all users concerned.

In this case, Article 5(1) requires the consent of "*all users concerned*", in other words, the two parties to a communication. Consent of one of the parties is not enough.

In the context of elaborating its Opinion 2/2006[42], the Article 29 Working Party looked into several services that entailed the screening of email content and, in some cases, the tracking of email opening. The Working Party expressed concern that in such services one of the communicating parties was not informed. For these services to be compliant with Article 5(1) consent of both communicating parties is necessary.

III.B.3 Articles 6(3), 9, 13 and 5(3) - Timing when consent is required

"*... having been provided with clear and comprehensive information, ...*"

Various provisions of the e-Privacy Directive contain either explicit or implicit language indicating that consent is to be provided prior to the processing. This is in line with Directive 95/46/EC.

Article 6(3) of the e-Privacy Directive includes an explicit reference to the prior consent of the subscriber or user concerned, laying down an obligation to provide information and obtain prior consent before processing traffic data for the purposes of marketing electronic communication services or value added services. For certain types of services, consent may be obtained from the subscriber at the moment of the subscription to the service. In other cases, it may be feasible to obtain it directly from the user. A similar approach is followed under Article 9 regarding the processing of location data other than traffic data. The service provider must inform the users or subscribers - *prior to obtaining their consent* - of the type of location data other than traffic data, which *will be* processed. Article 13 sets forth a requirement to obtain prior consent from subscribers to use automatic calling systems without human intervention, fax or e-mail for purposes of direct marketing.

Article 5(3) contains a specific rule regarding the storing of information or gaining of access to information on a user's terminal, including for the purpose of tracking the user's on-line activities. While Article 5(3) does not use the word prior, this is a clear and obvious conclusion from the wording of the provision.

It makes good sense for consent to be obtained *prior* to the starting of the data processing. Otherwise, the processing carried out during the period of time from the moment the processing had started until the moment that consent had been obtained

[42] Opinion 2/2006 on privacy issues related to the provision of email screening services, adopted on 21.02.2006 (WP118).

would be unlawful because of lack of legal ground. Furthermore, in such cases, if the individual decided against consenting, any data processing that had already taken place would be unlawful for that reason as well.

It follows from the above that whenever consent is *required*, it must be prior to the data processing starting. The possibility of starting the processing without having obtained consent first is only lawful when the Data Protection Directive or the ePrivacy Directive, rather than requiring consent, provides an alternative ground and refers to the right to object to or refuse the processing. These mechanisms are clearly distinguished from consent. In these cases, the processing may have already started and the individual has the right to object or refuse it.

An example of this can be found in Article 5(3) of the former e-Privacy Directive, which said (emphasis added): "*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 should be compared with the new wording of Article 5(3) of the e-Privacy Directive as amended by Directive 2009/136/EC[43], which states 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 (...)*". The consequences of this change in the wording of Article 5(3) have been explained by the Article 29 Working Party in its opinion 2/2010 on online behavioural advertising[44]. The difference between refusal and consent is also further developed in the next chapter.

In many cases where the e-Privacy Directive or the Data Protection Directive provides for a possibility to refuse the processing of personal data, it is because the legal basis for the initial data processing is based on legal grounds *other* than consent, such as an existing contract. This is further illustrated in the next section, which comments on Article 13 of the e-Privacy Directive.

III.B.4. Article 13(2-3) - right to object and its distinction from consent

"…customers clearly and distinctintly are given the opportunity to object …"

Article 13 of the e-Privacy Directive foresees the use of consent to send electronic communications for direct marketing purposes lawfully. It does so by relying on a standard principle and a specific provision.

---

43 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws Text with EEA relevance, *O. J. L 337 , 18/12/2009 P. 0011 - 0036*

44 Opinion of 22 June 2010, WP 171: the issue whether consent may be expressed via "the appropriate settings of a browser or other application" [recital 66 of directive 2009/136/EC] is explicitly dealt with in point 4.1.1 of WP 171.

Regarding the use of automated calling machines, fax machines and email, it requires the prior consent of the data subject.

If the addressee of the commercial communication is an existing client and the communication aims at promoting the provider's own or similar products or services, the requirement is not consent, but ensuring that individuals *"are given the opportunity to object"* ex Article 13(2). Recital 41 explains the reasoning why the legislator, in this case, did not require consent: *"Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services"*. Thus, in principle, the contractual relationship between the individual and the service provider is the legal ground that allows the first contact by email. However, individuals should have the opportunity to object to further contacts. As the Working Party has already indicated: *"This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal"*.[45]

The need for consent should be distinguished from this right to object. As illustrated above in Chapter III.A.2, consent based on the lack of individuals' action, for example, through pre-ticked boxes, does not meet the requirements of valid consent under the Directive 95/46/EC. The same conclusion applies to browser settings which would accept by default the targeting of the user (through the use of cookies). This is made clear in the new wording of Article 5(3) quoted *supra* in Chapter III.B.3. These two examples fail to meet in particular the requirements for an unambiguous indication of wishes. It is essential that the data subject is given the opportunity to make a decision and to express it, for instance by ticking the box himself, in view of the purpose of the data processing.

In its opinion on behavioural advertising, the Working Party has concluded that "*it seems of paramount importance for browsers to be provided with default privacy-protective settings. In other words, to be provided with the setting of 'non-acceptance and non-transmission of third party cookies'. To complement this and to make it more effective, the browsers should require users to go through a privacy wizard when they first install or update the browser and provide for an easy way of exercising choice during use*"[46].

III.B.5. Articles 6.3, 9.3-4. - possibility to withdraw consent

"… possibility to withdraw consent at any time …"

The possibility to withdraw consent, which is implicit in Directive 95/46/EC, is taken up in various provisions of the e-Privacy Directive. This was explicitly stated in the Working Party's Opinion on the use of location data with a view to providing value added services[47]:

[45] Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, adopted on 27.02.2004.

[46] Opinion of 22.06. 2010, WP 171, op.cit.

[47] Opinion 5/2005 on the use of location data with a view to providing value-added services, adopted on 25.11.2005 (WP115).

"*Under Article 9 of Directive 2002/58/EC, people who have given their consent for the processing of location data other than traffic data may withdraw consent at any time and must have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data. The Working Party regards these rights — which can be taken as implementing the right to object to the processing of location data — as essential given the sensitive nature of location data. The Working Party believes that it is a precondition for the exercise of these rights that individuals are kept informed, not only when they subscribe to a service but also when they use it. Where a service requires ongoing processing of location data, the Working Party takes the view that the service provider should regularly remind the individual concerned that his or her terminal equipment has been, will be or can be located. This will allow that person to exercise the right to withdraw under Article 9 of Directive 2002/58/EC, should he or she wish to do so.*"

As already mentioned above, this implies that withdrawal is exercised for the future, not for the data processing that took place in the past, in the period during which the data was collected legitimately. Decisions or processes previously taken on the basis of this information can therefore not be simply annulled. However, if there is no other legal basis justifying the further storage of the data, they should be deleted by the data controller.

IV. Conclusions

This opinion looks into the legal framework regarding the use of consent under Directive 95/46/EC and Directive 2002/58/EC. The goal of this exercise is twofold: First, it aims to clarify the existing legal requirements and illustrate how they work in practice. At the same time, in doing so, it provides a reflection on whether the existing framework remains suitable in the light of the many new ways of processing personal data or whether changes to it may be necessary.

IV.1. Clarification of the key aspects of the current framework

Article 2 (h) of Directive 95/46/EC defines consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". Article 7 of the Directive, which sets forth the legal basis for processing personal data, sets out *unambiguous* consent as one of the legal grounds. Article 8 requires *explicit* consent as a legal ground to process sensitive data. Article 26.1 of Directive 95/46/EC and various provisions of the ePrivacy Directive require consent to carry out specific data processing activities within their scope of application. The points developed in this opinion aim at clarifying the various elements of this legal framework in an effort to make it easier to apply by stakeholders in general.

Elements/observations of general nature

- Consent is one of the six legal grounds to process personal data (one of five for sensitive data); it is an important ground as it gives some control to the data subject with regard to the processing of his data. The relevance of consent as an enabler of the individual's autonomy and self-determination relies on its use in the right context and with the necessary elements.

- Generally speaking, the legal framework of Directive 95/46/EC applies whenever consent is sought, independently of whether this happens off-line or on-line. For example, the same rules apply when a bricks and mortar retailer seeks sign up for a loyalty card scheme via a paper form, as would be the case if it did this through its Internet site. In addition, the ePrivacy Directive specifies certain data processing operations which are subject to consent: they mostly relate to the processing of data in connection with the provision of publicly available electronic communication services. The requirements for consent to be valid within Directive 2002/58/EC are the same as under Directive 95/46/EC.

- Situations where data controllers use consent as a legal ground to process personal data should not be confused with situations where the controller bases the processing on other legal grounds which entail an individual right to object. For example, this may be the case when the processing relies on the 'legitimate interests' of the data controller ex Article 7(f) of Directive 95/46/EC, yet the individual has the right to object ex Article 14(a) of Directive 95/46/EC. Another example is when a data controller sends e-mail communications to existing clients in order to promote the data controller's own or similar products or services, however, individuals have a right to object under Article 13.2 of Directive 2002/58/EC. In both cases, the data subject has the right to object to the processing, this is not the same as consent.

- Reliance on consent to process personal data does not relieve the data controller from his obligation to meet the other requirements of the data protection legal framework, for example, to comply with the principle of proportionality under Article 6.1(c), security of the processing *ex* Article 17, etc.

- Valid consent presupposes individuals' capacity to consent. Rules regarding the capacity to consent are not harmonised and may therefore vary from Member State to Member State.

- Individuals who have consented should be able to withdraw their consent, preventing further processing of their data. This is confirmed also under the ePrivacy Directive for specific data processing operations based on consent, such as the processing of location data other than traffic data.

- Consent must be provided before the processing of personal data starts, but it can also be required in the course of a processing, where there is a new purpose. This is stressed in various provisions of Directive 2002/58/EC, either through the requirement "prior" (e.g. Article 6.3) or through the wording of the provisions (e.g. Article 5.3).

Specific elements of the legal framework related to consent

- For consent to be valid, it must be *freely given*. This means that there must be no risk of deception, intimidation or significant negative consequences for the data subject if he/she does not consent. Data processing operations in the employment environment where there is an element of subordination, as well as in the context of government services such as health may require careful assessment of whether individuals are free to consent.

- Consent must be *specific*. Blanket consent without determination of the exact purposes does not meet the threshold. Rather than inserting the information in the

general conditions of the contract, this calls for the use of specific consent clauses, separated from the general terms and conditions.

- Consent must be *informed*. Articles 10 and 11 of the Directive lists the type of information that must necessarily be provided to individuals. In any event, the information provided must be sufficient to guarantee that individuals can make well informed decisions about the processing of their personal data. The need for consent to be "informed" translates into two additional requirements. First, the way in which the information is given must ensure the use of appropriate language so that data subjects understand what they are consenting to and for what purposes. This is contextual. The use of overly complicated legal or technical jargon would not meet the requirements of the law. Second, the information provided to users should be clear and sufficiently conspicuous so that users cannot overlook it. The information must be provided directly to individuals. It is not enough for it to be merely available somewhere.

- As to how consent must be provided, Article 8.2(a) requires *explicit* consent to process sensitive data, meaning an active response, oral or in writing, whereby the individual expresses his/her wish to have his/her data processed for certain purposes. Therefore, express consent cannot be obtained by the presence of a pre-ticked box. The data subject must take some positive action to signify consent and must be free not to consent.

- For data other than sensitive data, Article 7(a) requires consent to be *unambiguous.* "Unambiguous" calls for the use of mechanisms to obtain consent that leave no doubt as to the individual's intention to provide consent. In practical terms, this requirement enables data controllers to use different types of mechanisms to seek consent, ranging from statements to indicate agreement (express consent), to mechanisms that rely on actions that aim at indicating agreement.

- Consent based on an individual's inaction or silence would normally not constitute valid consent, especially in an on-line context. This is an issue that arises in particular with regard to the use of default settings which the data subject is required to modify in order to reject the processing. For example, this is the case with the use of pre-ticked boxes or Internet browser settings that are set by default to collect data.

IV.2 Assessment of the current framework and possible need for changes

Overall assessment

The Working Party considers that the current data protection framework contains a well-thought out set of rules that establish the conditions for consent to be valid in order to legitimise data processing operations. These apply in both the off- and on-line environments. More particularly:

The framework successfully achieves the balancing of a number of concerns. On the one hand, it ensures that only true, informed, consent is deemed as such. In this regard, Article 2(h) explicitly requiring consent to be freely given, specific and informed, is relevant and satisfactory. On the other hand, this requirement is not a straight jacket but it rather provides sufficient flexibility, avoiding technologically specific rules. This is illustrated in the same Article 2(h) where it defines consent as any indication of the individual’s wishes. This provides sufficient leeway in terms of the ways in which such

an indication can be provided. Articles 7 and 8, requiring respectively unambiguous and explicit consent, capture well the need for a balance between the two concerns, giving flexibility and avoiding overly rigid structures while guaranteeing protection.

The result is a framework which, if properly applied and implemented, is capable of keeping pace with the wide variety of data processing operations that often result from technological developments.

In practice however, establishing when consent is needed and more particularly the requirements for valid consent, including how to apply them concretely, is not always easy because of a lack of uniformity across Member States. Implementation at national level has resulted in different approaches. More specific shortcomings were identified during the discussions in the Article 29 Working Party that led to this Opinion, further described below.

Possible changes

- The notion of unambiguous consent is helpful for setting up a system that is not overly rigid but provides strong protection. While it has the potential to lead to a reasonable system, unfortunately, its meaning is often misunderstood or simply ignored. While the indications and examples developed above should contribute to enhancing the legal certainty and protection of individuals' rights when consent is used as a legal basis, the above situation seems to call for some amendments.
- More particularly, the Article 29 Working Party considers that the wording itself ("unambiguous") would benefit from further clarification as a part of the revision of the general data protection framework. Clarification should aim at emphasizing that unambiguous consent requires the use of mechanisms that leave no doubt of the data subject's intention to consent. At the same time it should be made clear that the use of default options which the data subject is required to modify in order to reject the processing (consent based on silence) does not in itself constitute unambiguous consent. This is especially true in the on-line environment.
- In addition to the clarification described above, the Article 29 Working Party suggests the following:

    i. *First*, include in the definition of consent of Article 2(h) the word "unambiguous" (or equivalent) in order to reinforce the notion that only consent that is based on statements or actions to signify agreement constitutes valid consent. In addition to adding clarity, this would align the concept of consent under Article 2(h) with the requirements for valid consent under Article 7. Moreover, the meaning of the word "unambiguous" could be further explained in a recital of the future legal framework.

    ii. *Second*, in the context of a general accountability obligation, the controllers should be in a position to demonstrate that consent has been obtained. Indeed, if the burden of proof is reinforced so that data controllers are required to demonstrate that they have effectively obtained the consent of the data subject, they will be compelled to put in place standard practices and mechanisms to seek and prove unambiguous consent. The type of mechanisms will depend on the

context and should take into account the facts and circumstances of the processing, more particularly its risks.

- The Article 29 Working Party is not convinced that the legal framework should require explicit consent as a general rule for all types of processing operations, including those currently covered by Article 7 of the Directive. It considers that unambiguous consent which encompasses explicit consent but also consent resulting from unambiguous *actions* should remain the required standard. This choice gives more flexibility to data controllers to collect consent and the overall procedure may be quicker and more user friendly.

- Several aspects of the legal framework that apply to consent are deduced from the wording, legal history or have been developed through case law and Article 29 Working Party Opinions. It would provide more legal certainty if such aspects were expressly built in the new data protection legislative framework. The following points could be taken into account:

    i. The inclusion of an express clause setting up the right of individuals to withdraw their consent.

    ii. The reinforcement of the notion that consent must be given before the processing starts, or before any further use of the data for purposes not covered by an initial consent, where there is no other legal ground for the processing.

    iii. The inclusion of explicit requirements regarding the quality (obligation to provide information on data processing in a manner which is easy to understand, in clear and plain language) and accessibility of the information (obligation for the information to be conspicuous, prominent and directly accessible). This is vital for enabling individuals to make informed decisions.

- Finally, with regard to individuals lacking legal capacity, provisions ensuring enhanced protection could be foreseen, including:

    i. Clarifications as to the circumstances in which consent is required from parents or representatives of an incapable individual, including the age threshold below which such consent would be mandatory.

    ii. Laying down the obligation to use age verification mechanisms, which may vary depending on circumstances such as the age of children, the type of processing, whether particularly risky, and whether the information will be kept by the data controller or made available to third parties;

    iii. A requirement for information to be adapted to children insofar as this would make it easier for children to understand what it means when data from them are collected, and thus deliver consent;

    iv. Specific safeguards identifying data processing activities, such as behavioural advertising, where consent should not be a possible basis to legitimise the processing of personal data.

The Article 29 Working Party will revisit the issue of consent. More particularly, national data protection authorities as well as the Working Party may decide at a later stage to draft guidelines to developing this Opinion further, providing additional practical examples related to the use of consent.

Done in Brussels, on 13 July 2011

For the Working Party
The Chairman
Jacob KOHNSTAMM