Consent, its modalities, dynamics and record-keeping

Received: 31st May, 2017

Georg Philip Krog
is co-founder, Chief Privacy Officer & General Counsel of Signatu. His previous roles include consultant in data protection law, copyright law and private international law, researcher at the Faculty of Law in Oslo and Max Planck Institut in Hamburg, and Fulbright Scholar at Harvard Law School and Stanford Law School.

Signatu AS, Oslo Science Park, Gaustadaleén 21, 0349 Oslo, Norway
E-mail: georg@signatu.com

Abstract The paper provides a general introduction to consent as a legal basis for processing personal data; the definition, modalities and dynamics of consent; the data controller's obligation to enable the data subject to exercise his or her legal power to grant, to refuse or to terminate any permission granted to the data controller with respect to processing the data subject's personal data; and the data controller's obligation to demonstrate consent. The paper demonstrates that, through the concept of legal power, result declarations and temporal characterisations of legal effects, one can model, engineer and design systems with actions that perform, give effect to, enforce and record a data subject's power and declarations to grant permission, to refuse to grant permission or to terminate any permission previously granted to the data controller with respect to processing the data subject's personal data.

KEYWORDS: consent, consent management, consent records, GDPR

INTRODUCTION

Under the conditions set out in the General Data Protection Regulation (GDPR), data controllers must obtain valid, demonstrable consent from data subjects before processing their personal data.

This paper provides a general introduction to consent as legal basis for processing personal data; the definition, modalities and dynamics of consent; the data controller's obligation to enable the data subject to exercise his or her legal power to grant permission, to refuse to grant permission or to terminate any permission previously granted to the data controller with respect to processing the data subject's personal data; and the data controller's obligation to demonstrate consent.

The paper will demonstrate that through the concept of legal power, result declarations and temporal characterisations of legal effects, one can model, engineer and design systems with actions that perform, give effect to, enforce and record a data subject's power and declarations to grant, to refuse and to terminate any permission granted to the data controller with respect to processing the data subject's personal data.

LEGAL BASIS

The GDPR, if applicable, permits a controller to process a data subject's personal data only if the processing of the personal data has a specific lawful basis.

One such lawful basis is the data subject's permission that a controller may process the data subject's ordinary personal data and/or special personal data, as provided for in GDPR Article 6.1 (a) and Article 9.2 (a) respectively. The data subject can also permit the data controller to transfer the data subject's personal data to a third country or an international organisation, as provided for in GDPR Article 49.1 (a), or permit a controller to carry out automated decision making, as provided for in GDPR Article 22.2 (c) and 22.4, or permit a controller to process restricted personal data, as provided for in GDPR Article 18.2. GDPR Article 9.2 (a) (and Article 22.4 ref. Article 9.2 (a)) and Article 49.1 (a) require the explicit consent of the data subject.

DEFINITION, MODALITIES AND DYNAMICS OF CONSENT

GDPR Article 4(11) provides the following definition of consent:

> 'For the purposes of this Regulation: "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

The normative modalities of consent would be captured by saying that a data subject's right to grant a data controller permission to process his or her personal data is equivalent to the data controller having no right to process (or not to process) the data subject's personal data.

From the data controller's perspective, the permission that the data subject has granted the data controller to process the data subject's personal data is equivalent to saying that the data controller has a privilege, a permissive right and a mere liberty right toward the data subject to process (or not to process) the data subject's personal data.[1]

The dynamics of consent would be captured by saying that (in a legal capacity) the data subject holds the power to grant permission, to not grant permission or to terminate any permission previously granted to the data controller with respect to processing the data subject's personal data through any action that grants, does not grant or terminates the permission and its legal effect. Hence, one can say that the data subject's performance of an action grants or terminates the permission (vis-à-vis the data controller processing the data subject's personal data) and its legal effect which the data subject pursues in his or her own interest, or one can say that the data subject may grant or terminate the permission (vis-à-vis the data controller processing the data subject's personal data) and its legal effect through the action.

This is equivalent to saying that the data controller is subject to and is not immune from the data subject's power to permit (or to refuse or terminate) the permission toward the data controller with respect to processing the data subject's personal data, and that if the data controller obstructs the data subject from exercising that power, then the data controller enables his/her immunity from the data subject's power.

As the data controller can interfere with the data subject's effective exercise of this power, the GDPR imposes obligations on the data controller to make that power effective. Further conditions for the validity, formation or effect of a contract are regulated under member state law, which is outside the scope of the present paper (see GDPR Article 8.1).

OBLIGATIONS TO ENABLE THE DATA SUBJECT TO GRANT OR TERMINATE THE PERMISSION

The GDPR imposes obligations on the data controller to enable the data subject to exercise their power through which the data subject grants, refuses or terminates permission for the data controller to process the data subject's personal data, and its legal effect, which in turn enables the data subject to pursue his or her own interest.

If the data controller does not perform the obligations to enable the data subject to exercise their power to grant, refuse or terminate the permission, then the conditions set out in the GDPR to achieve valid consent are not fulfilled and the data controller lacks the permissive right to process the data subject's personal data, and corresponding sanctions can be activated.

The obligation to enable the data subject to exercise his or her power to grant, refuse or terminate this permission is discussed in the following sections.

Enable the data subject to understand s/he can perform his/her power at any time

For consent to be a lawful basis for the processing of personal data under the GDPR, the data controller is obliged to inform the data subject that the data subject may at any time grant, refuse or terminate permission for the data controller to process the data subject's personal data (GDPR Article 7.3, first and third sentence).

Enable the data subject to understand through which actions s/he has the power to grant, refuse or terminate the permission

For consent to be a lawful basis for the processing of personal data under the GDPR, the data controller is obliged to inform the data subject about the actions the data subject may take to grant, refuse or terminate permission for the data controller to process the data subject's personal data (GDPR Article 4(11) and 7.3, first sentence).

Unambiguous statement or action

The GDPR obliges the data controller to use statements and/or actions that enable the data subject to grant, refuse or terminate the permission for the data controller to process the data subject's personal data, and requires both statements and/or actions to be unambiguous (GDPR Article 4(11). A statement or action through which the data subject starts the permission is unambiguous according to a literal understanding if the statement or action is not open to more than one interpretation and that statement signifies agreement to the processing (WP29, Opinion 15/2011[2]). According to GDPR Recital 32, an action that affirms consent to the processing of personal data can be 'conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data'.[3]

Statement

According to the compromise embodied in GDPR Article 4(11), the data controller's request for consent may be a request in which the data subject's 'unambiguous indication … by a statement' signifies agreement to the processing of the data subject's personal data. According to GDPR Recital 32, a statement that affirms agreement to the processing of personal data can be 'a written statement including by electronic means, or an oral statement … which (when eg visiting an internet website) clearly indicates (the) context (of) the data subject's acceptance of the proposed processing of his or her personal data'. GDPR Recital 32 provides that a statement 'could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement' and thus counts ticking unchecked opt-in boxes as statements. If a data subject does not uncheck a pre-checked opt-in tick box, then the data subject does not affirm agreement according to GDPR Recital 32, which provides that 'pre-ticked boxes … should not … constitute consent'.

Action

According to the compromise embodied in GDPR Article 4(11), the data controller's request for consent can be a request in which the data subject's 'unambiguous indication … by a clear affirmative action' signifies agreement to the processing of the data subject's personal data. The literal meaning of the term 'clear affirmative action' is that it is easy to understand if and how an action affirms consent to the processing of personal data. If, on the one hand, the data subject omits to give an indication to signify agreement, then GDPR Recital 32 provides that 'silence … or inactivity should not … constitute consent'. Silence or inactivity has inherent ambiguity (the data subject might have meant to assent or might merely have meant not to perform the action) (WP 29, Opinion 5/2004[4]). If, on the other hand, the data subject acts to give an indication to signify agreement, then the data controller must qualify those acts that count as acts to unambiguously (and explicitly if needed) signify agreement.

Explicit consent

For consent to be a lawful basis for the processing of personal data under GDPR Article 4(11), the GDPR requires explicit consent for the processing of sensitive personal data (GDPR Articles 9.2 (a)) and for transfers of personal data to a third country or an international organisation (GDPR 49.1 (a)). The GDPR does not require explicit consent for ordinary personal data (GDPR Article 6.1 (a)) (WP29, Opinion 15/2011[5]). The GDPR does not define the term 'explicit' consent. A literal understanding of the term 'explicit' consent is that the consent must be stated expressly in words (whether oral or written) clearly and in detail, leaving no room for confusion or doubt. Hence, the data subject's consent for sensitive data and for the transfer of data to a third country or an international organisation must be affirmed in a clear statement (whether oral or written), and the data subject's consent for ordinary data must be affirmed in a statement or clear affirmative action. The requirement for explicit consent means that consent that is inferred will not meet the requirement of GDPR Articles 9.2 (a) and 49.1 (a).

Enable the data subject to understand the content of the permission request

The two types of consent are described below.

Consent is informed

For consent to be a lawful basis for the processing of personal data under the GDPR, the data controller is obliged to present and provide the information in the consent request with a degree of quality that enables the data subject to be 'informed', per GDPR Article 4(11).

According to a literal understanding, an 'informed' indication of the data subject granting the data controller permission to process the data subject's personal data means that the data subject has or shows knowledge of the data controller's processing and the consequences of consenting to the data controller's processing.

According to GDPR Recital 42, 'the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended'. According to a literal understanding, 'aware' means having knowledge or perception of a situation or fact.

The obligation on the data controller to inform the data subject can be further developed.

First, for consent to be a lawful basis for the processing of personal data under GDPR Article 4(11), the amount of information in the data controller's consent request should not be so extensive that the data subject chooses not to inform himself or herself; at the same time, it should include all information that the data controller is obliged to provide to the data subject.

Second, for consent to be a lawful basis for the processing of personal data under the

GDPR, the data controller's consent request must meet the language demands of the GDPR. GDPR Recital 32 provides that 'if the data subject's consent is to be given following a request by electronic means, the request must be clear, concise'.

Further, GDPR Recital 42 provides that 'in accordance with Council Directive 93/13/EEC (1) a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language'.

Furthermore, GDPR Recital 58 provides that 'the principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language … be used'.

If the data controller requests the data subject's consent in the context of a written declaration which also concerns other matters, then GDPR Article 7.2 obliges the data controller to present the request for consent 'in an intelligible and easily accessible form, using clear and plain language'. GDPR Recital 39 provides that 'the principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used'.

In the UK, the Information Commissioner's Office (ICO) recently published draft guidance on consent. It states that 'if the request for consent is vague, sweeping or difficult to understand, then it will be invalid. In particular, language likely to confuse — for example, the use of double negatives or inconsistent language — will invalidate consent' and that 'there is a tension between ensuring that consent is specific enough and making it concise and easy to understand.[6] In practice this means you may not be able to get blanket consent for a large number of parties, purposes or processes. This is because you won't be able to provide prominent, concise and readable information that is also specific and granular enough'.

The GDPR does not explicitly deal with grammatical issues of the language to be used in consent requests, that is, how to combine the terms to write correct and meaningful sentences. However, the GDPR does require the language used in communications with data subjects to be intelligible. A rough simplification of language properties may give ideas for how to author a consent request.

Roughly speaking, natural language can be described in four dimensions by saying that natural language is more or less precise (the degree to which the meaning of a text in a certain language can be directly retrieved from its textual form), expressive (the range of propositions that a certain language is able to express), natural (how close the language is to a natural language in terms of readability and understandability to speakers of the given natural language) and simple (the simplicity or complexity of an exact and comprehensive language description covering syntax and semantics).

Understanding the correlations between the dimension pairs of a natural language may give further ideas regarding how to author a consent request. Precision and simplicity often exhibit a strong negative correlation (precise language tends to be complex and not simple), where expressiveness and simplicity often exhibit a strong negative correlation (expressive languages tend to be complex and not simple), where naturalness and expressiveness often exhibit a strong positive correlation (naturalness of language tends to be complex), where naturalness and simplicity often exhibit a strong negative correlation (naturalness of language tends to be complex and not simple), where precision and naturalness often exhibit a less negative correlation (precise language tends to be natural) and where precision and expressiveness often exhibit a less negative correlation (precise language tends to be expressive).

Third, for consent to be a lawful basis for the processing of personal data under the GDPR, the data controller's consent request must be 'intelligible' (GDPR Recital 42) and 'easy to understand' (GDPR Recital 39 and 58). The wording seems to indicate that these notions do not refer to the intention of the author (ie controller) of the consent request, and do not refer to specific legal or contractual rules that a consent request of a certain type counts as intelligible, and do not refer to the meaning that is usually given to consent requests of a certain kind, but rather refer to the way in which the consent request and its context have, or should have been, perceived by the data subject. Hence, the author (controller) of the consent request must anticipate how the data subject will perceive the consent request.

Consent is specific

For consent to be a lawful basis for the processing of personal data under GDPR Article 4(11), the data controller is obliged to present and provide the information in the consent request with a degree of precision that enables the data subject to grant the data controller permission to process the data subject's personal data on the basis of purposes that are 'specific' (WP29, Opinion 15/2011[7]).

Whereas the requirement for consent to be 'informed' relates predominantly to the quality (preciseness, expressiveness, naturalness and simplicity) of the information in the consent request, the requirement for consent to be 'specific' relates to the information that is required to present in the consent request and how that information is linked.

According to a literal understanding, 'specific' indication that signifies consent to the processing means that the indication signifies consent to some specific information that belongs to the consent request and not referred to from the request and that specifies how the elements of the data processing are linked (Court of Justice in cases C-397/01 to C-403/01[8]).

The GDPR gives hints about which information to include in the consent request. GDPR Recital 42 provides that 'for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended'. GDPR Recital 39 provides that the principle of transparency 'concerns, in particular, information to the data subjects on the identity of the controller … to ensure fair and transparent processing in respect of the natural persons concerned'. GDPR Recital 32 provides that 'consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them'.

The GDPR also gives hints about how the information in the consent request should be linked. GDPR Recital 43 provides that 'consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance'. Hence, to fulfil the requirements of a 'specific' consent, the consent request must correctly specify how the elements of the data processing are linked (eg how, where and why personal data are processed).

Requesting consent by a measure

For consent to be a lawful basis for the processing of personal data under the GDPR, the data controller may be obliged to provide the consent request by a measure that is appropriate, similar to the requirement in GDPR Article 12.1, which obliges the data controller to 'take appropriate measures to provide any information referred to in Articles 13 and 14'. Which measure is appropriate must be answered in relation to the context in which the request takes place.

Enable the data subject to understand the legal effect of the actions s/he has the power to perform

For consent to be a lawful basis for the processing of personal data under the GDPR, the data controller is obliged to inform the data subject that if the data subject terminates the permission, then it shall not affect the lawfulness of processing based on consent before its withdrawal (GDPR Article 7.3, second sentence).

Enable the data subject to exercise his/her power freely

For consent to be a lawful basis for the processing of personal data under the GDPR, the data controller is obliged to enable the data subject to freely exercise his/her power to grant, refuse or terminate the permission for the data controller to process the data subject's personal data (GDPR Article 4(11).

According to a literal understanding, a free indication that signifies consent is a decision to agree that is not under the control or influence of the data controller. GDPR Recital 42 provides that 'consent should not be regarded as freely given if the data subject has no genuine or free choice (to) consent'.

GDPR Recital 43 provides that 'consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance'. Hence, the consent request must correctly specify how the elements of the data processing are linked (eg how, where and why etc the personal data are processed) and provide separate consent to be given to different personal data processing operations.[9]

GDPR Recital 42 provides that 'consent should not be regarded as freely given if the data subject … is unable to refuse … consent without detriment'.[10] The notion 'detriment' means a cause of harm or damage. Hence, consent can be considered to be invalid if refusing consent causes harm or damage to the data subject.

GDPR Article 7.4 provides that 'when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract'. GDPR Recital 43 provides that 'consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance'. Hence, consent should not be bundled with a condition of the performance of a contract.

GDPR Recital 43 provides that 'in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation'.

From a rights perspective, one may question whether a data subject wishes to consent to a data controller's consent request in order to enable himself/herself to achieve the legal effect of the privacy notice if the permission disadvantages the data subject's interests or if the permission gives the data controller a permissive right towards the data subject that promotes, advances or satisfies controller's interest for the sole benefit of the data controller. In its Opinion 15/2011 regarding the Data Protection Directive, WP29 states that 'consent should refer to the processing that is reasonable and necessary in relation to the purpose' and that falls 'within the reasonable expectations of the data subject'. A data subject's reasonable expectations may be based on the relationship with the data controller, the legitimacy of controller's processing purposes, whether the data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for a specific purpose may take place.

The action to request permission 'must be … not unnecessarily disruptive to the use of the service for which it is provided' (GDPR Recital 32). If permission requests are unnecessarily disruptive, a data subject may grant permission without reading the consent request in order to pursue other interests (eg read an article on a newspaper website), which in turn would lead to uninformed consent.

Enable the data subject to grant, refuse or terminate permission at any time

For consent to be a lawful basis for the processing of personal data under the GDPR, the data controller is obliged to facilitate the means through which the data subject at any time can exercise his/her power to grant, refuse or terminate permission for the data controller to process the data subject's personal data by the actions described above (GDPR Article 7.3, first and third sentence).[11]

Authenticating the data subject to enable termination of permission

If the data controller bases the processing of a data subject's personal data on his or her consent and if the data subject performs the action to terminate the permission toward the data controller in accordance with GDPR Article 7.3, then the data controller must have evidence that enables them to verify whether or not the data subject has the right to terminate this permission. This implies that the data controller has an obligation to verify the identity of or authenticate the data subject.

By comparison, if the data controller is not in a position to identify the data subject when a data subject requests to perform his or her rights under GDPR Articles 15–22, then the data controller is exempted from exercising the rights in accordance with GDPR Article 12.2. This implies that the GDPR does not impose an obligation on the data controller to be able to identify and authenticate the data subject for the purpose of exercising his or her rights under GDPR Articles 15–22. GDPR Article 12.7 provides that 'without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject'.

In addition, GDPR Article 7.1 obliges the data controller to 'be able to demonstrate that the data subject has consented'. This means that the data controller is obliged to have a system of consent records that show that a specific data subject who can be authenticated has consented to the processing of his or her personal data.

The GDPR does not lay down prescriptive requirements on how to authenticate the data subject, but gives some general hints in Article 4(1), while GDPR Recital 64 provides that 'the controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers'.

OBLIGATION TO BE ABLE TO DEMONSTRATE CONSENT

GDPR Article 7.1 imposes an obligation on the data controller to 'be able to demonstrate' consent, which is echoed in Recital 42. The obligation is expressly limited to consent, however, a consent record should as a minimum be able to record that the data subject grants, refuses or terminates the permission toward the data controller as well as passivity as to any of these three actions.

The literal meaning of 'able' is to have the power, skill, means or opportunity to do something. Hence, if GDPR Article 7.1 obliges the data controller to have the power, skill, means or opportunity to demonstrate a data subject's consent to the processing of his or her personal data, then GDPR Article 7.1 also places a burden or an onus upon the data controller to have the measures for obtaining and recording the consent and to actually obtain and record the data subject's consent to the processing of his or her personal data. The GDPR does not expressly regulate how long the data controller must maintain the record of consent after consent was given.

A literal understanding of the expression 'be able to demonstrate' does not mean that the data controller is actually obliged to demonstrate the existence of a data subject's consent to the processing of his or her personal data. However, some commentators suggest that if a data subject (or eg a data protection authority) offer *prima facie* evidence for a lack of or invalid consent, then the evidential burden of proof should *de facto* shift to the data controller.[12] The arguments that may justify this interpretation may be that (1) the data controller is best positioned to obtain and secure first-hand knowledge of consent; (2) the data controller understands how his/her system records the consent and is therefore best positioned to show the evidence; and (3) GDPR Article 7.1 seeks to protect the data subject (due to being generally considered as in the weaker position because of his or her procedural or socio-economic position) and presumes that data controller's obligation to demonstrate consent protects the data subject by rules on evidence more favourable to the data subject's interests than the general rules provide for (regardless of whether or not the data subject is a plaintiff or a defendant).

GDPR Article 7.1 specifies the scope of the data controller's ability to demonstrate consent by the expression 'that the data subject has consented to processing of his or her personal data'. This means that the consent record must record the consent interactions between the data subject and the data controller (and third-party controllers) with reference to the identities of the data controller and the data subject, the time of the start of the permission, the refusal of the permission or the termination of the permission, and the content of the permission request paired with the conditions for consent to enable proof of the validity of the claims that the GDPR conditions for consent are not fulfilled.

As the degree to which the data controller's evidence for valid consent can be trusted is equal to the degree to which the data controller can interfere with and change the evidence, one may question whether the measures to record consent are 'appropriate' according to GDPR Recital 78 only if the consent record provides tamper-proof and immutable evidence for the consent.

References and Notes

1. Sartor, G. (2006) 'Fundamental legal concepts: a formal and teleological characterisation', *Artificial Intelligence and Law*, Vol. 14, pp. 101–142.
2. WP29 states that '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'. See: WP29 (2011) 'Opinion 15/2011 on the definition of consent, regarding the

Data Protection Directive', 13th July, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (accessed 30th June, 2017).

3. The compromise reached in the final GDPR text is that 'consent (that) is to be given by data subjects remains 'unambiguous' for all processing of personal data … and that consent has to be 'explicit' for sensitive data'. See: Council of the European Union (2015) 'Consolidated text of the draft General Data Protection Regulation from the Council of the European Union to the Permanent Representatives Committee as an outcome of the final trilogue', available at: http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf (accessed 30th June, 2017). The Commission proposed initially explicit consent for personal data that are and are not sensitive 'to avoid confusing parallelism with "unambiguous" consent and in order to have one single and consistent definition of consent, ensuring the awareness of the data subject that, and to what, he or she gives consent'. See: European Commission (2012) 'Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', 25th January, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en (accessed 30th June, 2017).

4. WP29 has stated the unsuitability of consent based on individuals' silence in the context of sending direct marketing through e-mails: 'Implied consent to receive such mails is not compatible with the definition of consent of Directive 95/46/EC … Similarly, pre-ticked boxes, eg on websites are not compatible with the definition of the Directive either'. WP29 (2004) 'Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC', adopted on 27th February 2004 (WP90), available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp90_en.pdf (accessed 30th June, 2017).

5. In its Opinion 15/2011 regarding the Data Protection Directive, WP29 states that 'the requirement for explicit consent means that consent that is inferred will not normally meet the requirement of Art 8(2). WP29, ref. 2 above.

6. ICO (2017) 'Consent Guidance', available at: https://ico.org.uk/about-the-ico/consultations/gdpr-consent-guidance/ (accessed 30th June, 2017).

7. In its Opinion 15/2011 regarding the Data Protection Directive, WP29 states that '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'. WP29, ref. 2 above.

8. Regarding the Data Protection Directive, the Court of Justice insisted on this point in its 2004 judgment regarding an employment contract that included conditions which were not spelt out in the contract but only referred to. Judgment of the Court (Grand Chamber) of 5th October, 2004, Pfeiffer, Roith, Süß, Winter, Nestvogel, Zeller, Döbele in joined Cases C-397/01 to C-403/01, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0397 (accessed 30th June, 2017).

9. The Hungarian Data Protection Authority recently issued a guideline that says that if user consent is mandatory — such as in connection with the use of third-party cookies — then the website operator must obtain separate consent relative to the use of each relevant cookie. In such cases, the Hungarian DPA will not accept the website operator's bundling of consent covering multiple cookies at the same time. The DPA suggests that the website operator should implement a consent mechanism providing separate checkboxes for each relevant cookie. See: Hungarian Data Protection Authority (2017) 'Tájékoztató a webáruházak ra vonatkozó adatvédelmi követelményekról', available at: http://naih.hu/files/2017-02-17-webaruhaz-tajekoztato-NAIH-2017-1060-V.pdf (accessed 30th June, 2017).

10. 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'. See WP29 (2007), 'Working Document on the processing of personal data relating to health in electronic health records (EHR), WP131', available at: http://www.dataprotection.ro/servlet/ViewDocument?id=228 (accessed 30th June, 2017).

11. The Data Protection Authority of Hamburg recently issued a guideline that website owners using Google Analytics must inform website users

that Google Analytics process their personal data and that deactivation of Google Analytics is possible by providing links to opt out. See: Data Protection Authority of Hamburg (2017) 'Hinweise des HmbBfDI zum Einsatz von Google Analytics', available at: https://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_fuer_Webseitenbetreiber_in_Hamburg_2017.pdf (accessed 30th June, 2017).

12. Van Alsenoy, B. (2016) 'Liability under EU data protection law: from Directive 95/46 to the General Data Protection Regulation', point 3.1.3, available at: https://www.jipitec.eu/issues/jipitec-7-3-2016/4506 (accessed 30th June, 2017).