Comments on WP29 guidelines on consent

23rd January 2018

Comments on the Introduction

The guidelines state in the second paragraph on page 4 that:

"Consent remains one of six lawful bases to process personal data, as listed in Article 6 of the GDPR. When initiating activities that involve processing of personal data, a controller must always take time to consider whether consent is the appropriate lawful ground for the envisaged processing or whether another ground should be chosen instead."

We think the second sentence could possibly be interpreted as suggesting some kind of hierarchy between the bases, with consent needing to be considered in the first instance.

However, the guidelines state in the fourth paragraph on page 4 that:

"The existing Article 29 Working Party (WP29) Opinions on consent remain relevant, where consistent with the new legal framework, as the GDPR codifies existing WP29 guidance and general good practice and most of the key elements of consent remain the same under the GDPR. *Therefore, in this document, WP29 expands upon and completes earlier Opinions on specific topics that include reference to consent under Directive 95/46/EC, rather than replacing them."* [Our emphasis.]

We note in the context of the 1995 Directive that this question is referenced in Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7, where it is stated on page 10 that:

"Article 7 starts with consent and goes on to list the other grounds for lawfulness, including contracts and legal obligations, moving gradually to the legitimate interest test, which is listed as the last among the six available grounds. The order in which the legal grounds are listed under Article 7 has sometimes been interpreted as an indication of the respective importance of the different grounds. *However, as already emphasised in the Working Party's Opinion on the notion of consent, the text of the Directive does not make a legal distinction between the six grounds and does not suggest that there is a hierarchy among them*." [Our emphasis.]

We suggest that to avoid any confusion, a simple drafting solution would be to omit the second sentence (i.e. the sentence beginning 'When initiating activities…'), or to rephrase paragraph 2 of page for along the lines of:

"Consent remains one of six lawful bases to process personal data, as listed in Article 6 of the GDPR. When initiating activities that involve processing of personal data, **and if thinking about relying on 'consent' as the basis for processing,** a controller must always take time to consider whether consent is the appropriate lawful ground for the envisaged processing or whether another ground should be chosen instead."

Lastly, we note that the ePrivacy Regulation is still being negotiated and is subject to change. We recommend making this clearer in the guidelines, for example with an amendment to page 5 along the lines of the following:

"Meanwhile, WP29 is aware of the review of the ePrivacy Directive (2002/58/EC). **Although the ePrivacy Regulation is still being negotiated and its final requirements remain uncertain,** the notion of consent in the draft ePrivacy Regulation remains linked to the notion of consent in the GDPR. Organisations are likely to need consent under the ePrivacy instrument for most online marketing messages or marketing calls and

Association for Financial Markets in Europe
London Office: 39th Floor, 25 Canada Square, London E14 5LQ, United Kingdom T: +44 (0)20 3828 2700
Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 788 3971
Frankfurt Office: Skyper Villa, Taunusanlage 1, 60329 Frankfurt am Main, Germany T: +49 (0)69 5050 60590
www.afme.eu

online tracking methods including by the use of cookies or apps or other software. WP29 has already provided recommendations and guidance to the European legislator on the Proposal for a Regulation on ePrivacy."

Comments on section 2

We have no comments on this section.

Comments on section 3 Elements of valid consent

Section 3.1 Free/freely given

In example 1 on mobile apps, we think that the last sentence should read (with our emphasis): "If users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given."

Section 3.1.2 Conditionality

The first paragraph on page 9 states that:

"Article 7(4) GDPR indicates that, inter alia, the situation of "bundling" consent with acceptance of terms of conditions, or "tying" the provision of a contract or service to a request to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given."

The paragraph goes on to state that "…the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract."

We are not sure precisely what this sentence is intended to mean (in particular the expression "counter-performance of a contract").

We suggest that it should be clarified as to whether this is simply a restatement of the first part of the paragraph, or something different. We think that the intention is to clarify that personal data processing cannot be 'traded' for a service on the basis of consent. If we have understood the intended meaning correctly, the following drafting might be clearer:

"…the GDPR ensures that the processing of personal data for which consent is sought cannot **be treated as 'consideration' for a service under** ~~become directly or indirectly the counter-performance of~~ a contract."

With regard to the last paragraph on page 9, we note that Article 7(4) clarifies that it is seldom legitimate to make consenting to certain processing a prerequisite for obtaining a service when the processing is not necessary for the provision of the service. This is reasonable. However, the implication of this Article is that if the processing *is* necessary for the provision of the service, then consent can be legitimate.

Despite this, the Guidelines appear to state that, if the processing is necessary for contract performance then a data controller should not need to look to consent as a basis of processing. However, it is sometimes necessary to process *special category data* for the performance of a contract and it appears that the only legal basis under which this can be done is explicit consent.

This is particularly relevant in the case of health data, which is required for risk assessments needed in order to provide products like life insurance and 'lifetime' mortgage products.

If explicit consent cannot be relied on in this situation, this will have the effect of making it impossible to provide such services that *require* special category data unless an exemption under Article 9(2) (b – j) applies. This outcome does not appear to be intended under the GDPR.

In our view, in this context explicit consent should be valid, provided processing is very clearly explained and drawn to the attention of the data subject, along with the consequences of not consenting, as per the requirements in the guidelines.

Section 3.1.4 Detriment

This section clarifies that consent will not be the appropriate basis for processing in cases where only a 'downgraded service' will be provided if consent is refused or withdrawn. Related to our previous comments, in our view there is a difference between a controller offering only a *downgraded* service if consent to certain processing is not granted, as opposed to enabling a customer to obtain an *enhanced* service if the customer consents to additional optional data processing, particularly where that processing is necessary for the enhanced service to function.

An example of such an 'enhanced' service requiring more personal data than just a basic service could be a 'personalised' banking service that targets products and services based on the extra data collected. For example, a theoretical lifestyle app that (with consent) collects data about a user moving to a new house, or having a baby. The basic app could deliver information on mortgages, but the extra data would help the user to choose an area to live, or a school, etc. Similarly, the optional provision of additional health data by the user might enable more tailored product or service recommendations. This enhanced service would help a customer make important life decisions based on their particular circumstances.

Another example could be an enhanced, customised service for customers with a disability or health problem. Providing such a service could require the processing of health data. It would not be in data subjects' interests if controllers are unable to provide such enhancements due to an inability to rely on consent.

Section 3.3.1 Minimum content required for consent to be 'informed'

Broadly we agree with items (i) to (vi) in the guidelines. However, in respect of (i), we note that many businesses operate as groups of companies. As such, there may be multiple data controllers within a single business group. In this situation, providing a list of group entities receiving the data may be confusing for data subjects, who will seldom be interested in the firm's corporate structure, while the added length may lead to data subjects reading the consent text less thoroughly. An appropriately worded statement that the data will be shared with other group entities would generally be simpler and more engaging.

We note that under Articles 13 and 14, the fair processing information provided by the controller would need to name all of the controllers, but this would more appropriately be done in a second 'layer', rather than in the consent request itself.

Section 3.3.2 How to provide information

We suggest a drafting change on page 14, to say "Controllers cannot use long ~~illegible~~ privacy policies **which are difficult to understand**, or statements full of legal jargon."

Comments on section 4 Obtaining explicit consent

We suggest a drafting change on page 18, paragraph 3 to say "The GDPR prescribes that a ~~"clear affirmative act"~~ **"statement or clear affirmative action"** is a prerequisite for 'regular' consent." (i.e. to align with Article 4(11) GDPR).

The guidelines state on page 18 that:

"The term *explicit* refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent."

We note that Opinion 15/2011 states that (with our emphasis):

"…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. 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."

We understand from page 4 of the guidelines that Opinion 15/2011 remains valid.

We would therefore suggest that the guidelines on page 18 make reference to 'engaging in an affirmative action' as well as to 'an express statement of consent', and that a footnote be added to reference the quoted paragraph from Opinion 15/2011.

Furthermore, with regard to 'two stage verification' on page 19 we note that this process would disrupt the user journey. An additional email or message adds further to the risk of data subject information fatigue, particularly when it contains information that the data subject already received when providing the first consent.

Two stages are also not required under the GDPR text. In our view, a single step consent is adequate, provided it is appropriately clear, separate from other information, etc. Nonetheless, in situations where the process involves a consent that is combined with other matters or does not meet the requisite standard for some reason, a second stage (by email for example) would be a potential way to ensure that the appropriate standards for explicit consent are met.

We recommend amending page 19 of the guidelines as follows:

"**If for some reason the controller is concerned that an initial consent cannot reach the required explicit consent standard, as set out above, a 'two stage consent' can** ~~Two stage verification of consent can also~~ be a way to make sure explicit consent is valid. For example, a data subject receives an email..."

Comments on section 5 Additional conditions for obtaining valid consent

We have no comments on this section.

Comments on section 6 Interaction between consent and other lawful grounds in Article 6 GDPR

The guidelines state on page 22 that:

"As a general rule, a processing activity for one specific purpose cannot be based on multiple lawful bases. … the controller cannot swap between lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent."

We can envisage some practical situations where data may be initially processed for a specific purpose, and then the data controller will wish to (or indeed need to) process that same data for a new purpose (for example to manage litigation or to comply with a new legal obligation). In that case, the data controller would need to

establish a lawful basis for processing for the new purpose in a manner complying with the rules in Article 6(4), as well as Articles 13(3) and 14(4).

Establishing a lawful basis for the new purpose would not in our view be swapping between lawful bases for the original purpose (in the sense set out in the above paragraph). We think it would be useful for the guidelines to include clarification of this point.

As a more general point, we wish to highlight that in the area of financial services multiple bases for processing are likely to apply in some situations. In particular, firms must ensure that their contracts give effect to obligations imposed on them by law and regulatory guidance and must often conduct certain checks before entering into a contract (for example credit checks). In this situation 'performance of contract' or 'legal obligation' (or 'legitimate interests' in the case of regulatory guidance and 'soft law' obligations) might all be appropriate bases for processing. It would be helpful for the guidelines to recognise that some overlap may exist in such situations.

Comments on section 7 Specific areas of concern in the GDPR

Section 7.3 Data subject's rights

The guidelines state on page 29 that "Articles 16 to 20 indicate that when data processing is based on consent, data subjects have the right to erasure, the right to be forgotten when consent has been withdrawn and the rights to restriction, rectification and access."

Our understanding is that these rights are not limited to cases where data processing is based on consent.

We would therefore suggest amending the guidelines accordingly.

Comments on section 8 Consent obtained under Directive 95/46/EC

We have no comments on this section.

Contacts

Richard Middleton
Managing Director, Co-Head of Policy Division
AFME
T 020 3828 2709 | M 07 584 583 122
E richard.middleton@afme.eu

Walter McCahon
Policy Manager
UK Finance
T 020 3934 1131| M 07 725 683263
E walter.mccahon@ukfinance.org.uk