ETNO comments on the Article 29 Working Party Guidelines on Consent under Regulation 2016/679 (WP259)

On 28 November 2017, the Article 29 Working Party (WP29) adopted a set of Guidelines on Consent under Regulation 2016/67 and invited interested stakeholders to present comments. ETNO welcomes this opportunity to comment on WP29's guidelines and would like to stress the importance of clear rules on free and informed consent in order to ensure trust of individuals and data subjects.

ETNO particularly appreciates the clarification that all the references to the repealed Directive 95/46/EC in the existing e-Privacy Directive 2002/58/EC are to be understood as references to the GDPR. For ETNO members is it absolutely necessary to clarify the interplay between GDPR rules and current sector specific rules, especially in the transitory period when the GDPR will be applicable but the future e-Privacy Regulation will not yet be adopted and in force.

GENERAL COMMENTS

Consent is linked to Transparency as transparent information is required for the data subject to understand what he/she is consenting to. Consent must be user-focused and shall not result in confusion or mistrust. In this sense, the concept of consent information by layers is a good example by which companies comply with rules on consent and ensure that data subjects fully understands the proposed data processing and can require additional information if he/she considers it necessary. This provides users with the necessary information in order to comply with the law (freely given, specific, informed and unambiguous consent), but also to offer to those users who want to have additional information to obtain it in an easy and friendly way.

Empowerment is a key element for ETNO members, as companies want

- to put users in control of their data, strengthening their rights to privacy in line with GDPR and, at the same time,
- to unlock the value of personal data through new digital services that customers are demanding.

IS CONSENT ALWAYS THE BEST LEGAL GROUND?

WP29 Opinion on consent (WP 187 dated 13 July 2011) clearly stated that "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.

ETNO welcomes that WP29 reiterates this position in the new guidelines, stating that "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".

The use of consent "in the right context" is most relevant for ETNO members which are squeezed between GDPR and the current ePrivacy Directive and future ePrivacy Regulation. It is important that this approach is taken into account when assessing which are the adequate legal grounds for processing personal data in the framework of the ePrivacy debate.

On the statement in the guidelines that organisations are likely to need consent under the ePrivacy Regulation "for most online marketing messages or marketing calls, and online tracking methods including by the use of cookies or apps or other software", we would prefer that such assessment regarding the interplay between GDPR and ePR be done at a later stage, when the ePrivacy Regulation is adopted in its final form.

ELEMENTS OF VALID CONSENT

The key elements of the definition of consent (freely given, specific, and informed), as laid down in the repealed Directive 95/46/EC, remain valid in the GDPR. The novelty brought by the GDPR's definition is that valid consent must be "unambiguous" and involve a statement or a clear affirmative action from the data subject.

"Explicit" consent would only be requested for the processing of special categories of data and for automated decisions; with respect to other types of processing, consent has to be primordially **unambiguous**. In WP29's previous guidance on consent, the Working Party described the notion of "unambiguous" as leaving no doubt as to the individual's intention to deliver the consent. Nevertheless, unambiguous need not to be expressed. In ETNO's view, unambiguous consent can be inferred from certain actions.

Recital 32 already gives some examples on which form a "statement" or "clear affirmative action" could take: ticking a box when visiting an internet website (which, however, ETNO deems a form of explicit consent rather than unambiguous) or choosing technical settings for information society services. It must also be stressed that (as the WP29 suggests in Article 3(4) of the Guidelines) neither the GDPR nor its recitals give any indication that oral consent must necessarily be recorded. However, ETNO asks that the WP29 recognizes the validity of "pre-ticked" boxes when **these are** used as a means e.g. to remind data subjects in a clear and transparent way of their existing consent status with the controller, and the data subject is given an opportunity to review and amend that existing consent status by taking clear and affirmative action.

An example could be as follows:

> "Dear customer, as the tick box here indicates, you currently agree to receiving offers from us. Please check if you are still happy with this. You can make changes to your marketing preferences and confirm those changes".

In this context, the conduct of the data subject would clearly indicate the data subject's acceptance of the proposed processing of his or her personal data.

How consent has to materialise in practice should be decided by the controller, in full respect of the criteria established by the law. A one-size-fits-all solution should be avoided, since different industries may have different approaches to achieve the same objective efficiently.

GDPR already sets a high standard for consent. At this stage, it is worth reminding the basic principles of a valid consent:

- Consent should put individuals in control, build customer trust and engagement and enhance companies' reputation.
- Consent means offering individuals genuine choice and control.
- Consent must be specific, granular, clear and concise.
- Consent should be separate from other Terms and Conditions and should not be a precondition of a service.
- Consent can be withdrawn at any time and customers need to be informed about this right to withdraw and be provided with easy ways to withdraw consent at any time (art. 7 GDPR).

In addition, the conditions for informed consent include the existence of the right to withdrawal. ETNO would like clarification on how the user should be kept informed about this right (for example, whether it is sufficient to have a toggle visibly on or off, and to inform the data subject in privacy 'tours' in dashboard as well as in privacy notice about this option for withdrawal of consent

With regard to **granularity**, ETNO reinforces that it is important to find a balance between the need to ensure the freedom of the subject and to not increase disproportionately the amount of separate consents, leading to "consent fatigue". While we accept the principle of granularity, we are somewhat surprised by the concrete cases that are used as illustrations of granular and specific consent under Example 7 and Example 8. We do not contest that the purposes of on the one hand direct marketing to own customers and on the other hand sharing customer data within a group of companies (example 7) respectively allowing third parties to send targeted advertising (example 8) are different purposes. That said, we consider that direct marketing to own customers will in many circumstances not require consent but be based on the principle of legitimate interests. We therefore consider that the examples are not well chosen to illustrate the need for granularity and specificity of consent, and should better be replaced by more adequate examples.

With regard to **conditionality**, if for any reason the controller cannot offer the data subject a genuine choice, consent cannot be considered as an appropriate basis for processing. This is true when the controller would process the data under a different lawful ground after the data subject refused or withdrawn his consent. Also, consent should be separate from other Terms and Conditions and should not be a precondition of a service. With specific regard to Article 7(4), if the controller believes that the processing of data is necessary for the provision of the service, then the appropriate legal basis for such processing purpose should be the "performance of a contract". This holds true except when the controller still needs the subject's consent based on other purposes or rules (e.g., the e-Privacy Directive's conditions for electronic marketing).

ETNO members would like to have further clarifying examples with regards to Article 7(4) and the statement in the guidelines that "As the wording of Article 7(4) is not construed in an absolute manner, there might be very limited space for cases where this conditionality would not render the consent invalid." In addition, it is said in the guidelines that if a data-subject can "choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service that does not involve consenting to data use for additional purposes on the other hand", this constitutes genuine choice. ETNO members would like to have clarification on whether this apply for value-added services as defined in the ePrivacy Directive as well. Furthermore the statement

of WP29 does not address services, which are currently offered for free (in return for the use of data; e.g. a price draw to gather contact details of potential new customers). In most of these cases it will not be a viable alternative to offer an equivalent service which must not lead to any (reasonable) additional costs.

The WP29 guidelines note that consent must always be obtained before the controller starts processing personal data for which consent is needed. Clarification on the strictness of this requirement would be welcomed, for example regarding in-store situations where the customer asks for the best available tariff based on previous use. More specifically this regards whether it is possible to process the historical usage data needed, but only 'activate' the process of extracting the data when the data subject consents.

EXPLICIT CONSENT

If a controller wishes to process a special category of personal data, then it needs to comply with one of the conditions established in Article 9(2) GDPR. "Explicit consent" is one option for lawfully processing of a special category data.

Explicit consent is not defined in the GDPR, but must include all the conditions established for consent. There is therefore a possibility that the reader could be misled to believe that explicit consent is a separate concept from consent as defined in the GDPR. According to ETNO's understanding based on the draft guidelines, explicit consent must be affirmed in a clear statement, either oral or written. It should therefore be specified that an example of this type of consent can be to mark a checkbox is a mean whereby formal acceptance is manifested. Explicit consent should never be inferred in the same way as consent could be. It could be read similar to 'unambiguous' consent, for which it should be underlined that what is deemed to be unambiguous or explicit will depend on the case and context. Implied consent which is inferred from someone's actions cannot be explicit consent, however obvious it might be. ETNO is concerned about the guidelines' suggestion of obtaining explicit consent through a two stage verification as no viable options have been seen in a commercial online context (at least not in the telecom sector). ETNO would instead suggest to introduce procedures for sending out verifications of data subjects' consents in these particularly sensitive cases, and giving them an opportunity to object if they did not mean to consent or directing them to where they may withdraw their consent if they would like to do so.

ADDITIONAL CONDITIONS FOR VALID CONSENT

The GDPR's requirement is for a controller to be able to **demonstrate consent**. In practice, this involves a need to document every processing and to keep records to demonstrate what the individual has consented to, including the information he was given, and when and how he consented.

We however are of the view that organizations may choose to develop internal solutions or rely on independent third-party organizations to document all the processing and records in detail, as long as they are able to demonstrate consent. The solution chosen will depend on many factors such as the actual size of the organization, the nature of its core services, and other parameters.

Regarding how long proof should be kept, it should depend on the different circumstances around the specific data processing. The records should be kept as long as the processing is ongoing and as long as the controller could be held liable in case of breach of the law.

With regard to **withdrawal of consent**, if consent is withdrawn controllers must stop the processing as soon as possible based on the specific circumstances, unless the controller or processor can avail of another lawful basis, such as the compliance with a legal obligation or the protection of the vital interests of the data subject or another natural person. This would not affect the lawfulness of the processing. For any processing not based on consent, ETNO members are of the opinion that this can be specified in the privacy notice (and even the contract if this is the legal basis).

Controllers should always inform the data subject on his right of withdrawal at any time and in an easy way. For example, the organisation could provide an online form for withdrawing consent, available from an opt-out link at the bottom of every page.

The GDPR does not prevent a third party acting on behalf of an individual to withdraw their consent, but it needs to be ascertained that such third party has the authority to do so. This leaves the door open for sectorial opt-out registers or other broadly shared opt-out mechanisms, which could help demonstrate that consent is as easy to withdraw as it is to give.

INTERACTION BETWEEN CONSENT AND OTHER LAWFUL GROUNDS IN ARTICLE 6 GDPR

As previously stated, ETNO agrees with WP29 that a controller cannot continue to process the data for which consent were refused or withdrawn under a different legal basis as a backup, without giving the data subject a genuine choice on whether the processing shall continue based on that different legal basis.

CONSENT AND FURTHER PROCESSING FOR COMPATIBLE PURPOSES ARTICLE 6 (4) GDPR

Art. 29 WP outlines that "*if a controller processes data based on consent and wishes to process the data for a new purpose, the controller needs to seek a new consent from the data subject for the new processing purpose. The original consent will never legitimise further or new purposes for processing*".

According to Article 6 (4) GDPR further processing for a purpose other than that for which the personal data have been collected can either be based on consent or on Member State law. In the absence of these legal basis the controller must apply a compatibility test in compliance with the non-exhaustive criteria listed in Art. 6 (4) (a) – (e) GDPR. Recital 50 provides that no legal basis separate from that which allowed the collection of the personal data is required if the new purpose is compatible with the purpose for which the personal data were initially collected. The GDPR does not exclude consent nor any other legal basis for processing of personal data of Art. 6 (1) GDPR from the applicability of Art. 6 (4) GDPR.

As stated above, according to ETNO's understanding consent collected for initial processing of personal data can be a legal basis for further processing for compatible purposes in line with Art. 6 (4) GDPR. Therefore, ETNO asks for clarification on which kind of further processing the WP29 refers to.

Accordingly, the sentence "the original consent will never legitimise further or new purposes for processing" should be complemented with the specification "unless such further purpose is compatible with the purpose for which the personal data are initially collected."

With the same aim, the sentence at the end of par 3.4.1 should be modified to specify that "However, controllers do need to obtain a new and specific consent if purposes for data processing change after consent was obtained or if an additional *incompatible* purpose is envisaged".

SPECIFIC AREAS OF CONCERN IN THE GDPR

With regard to **children**, if an organization chooses to rely on children's consent they will need to implement age-verification measures and make "reasonable efforts" to verify parental responsibility for those under the relevant age. Our industry has been developing easy-to-use age and ID verification solutions that allow to verify both the real age of the data subject, and the truthfulness of the consent of the holder of parental responsibility. Authorities should rely on the solutions being developed by the industry.

The guidelines stipulate that Article 8 shall only apply when 1) the processing is related to the offer of information society services directly to a child, or 2) The processing is based on consent. ETNO members would like further clarity regarding whether this excludes the possibility of using this provision for electronic communications services.

The GDPR acknowledges in Recital 33 that if an organisation collects personal data for **scientific research**, it may not be able to fully specify its precise purposes in advance. ETNO believes there, as far as collecting personal data for scientific research is concerned, there is no need to be as specific as for other purposes. Controllers should identify the general areas of research and, where possible, give individuals granular options to consent only to certain areas of research or parts of research projects.

CONCLUSION

ETNO thanks Article 29 Working Party for this opportunity to provide comments on this important issue and calls for Article 29 Working Party to take a balance approach when adopting its final Guidelines on Consent. GDPR already sets a high standard for consent and its spirit of GDPR is to empower the data controller, based on the Accountability principle and a well understood Risk Based Approach.

As Art. 29 WP and EDPS have stated in several occasions, consent can be adequate in many contexts, but not always. Therefore, a risk-based approach as proposed by GDPR is more effective. The issue of consent within GDPR and consent within ePrivacy Regulation is especially important for ETNO members within the ongoing debate on the ePrivacy Regulation.