Position Paper

Bitkom views on Article 29 Working Party Draft Guidelines on Consent under Regulation 2016/679

23/01/2018

1. Introduction

Bitkom welcomes the opportunity to comment on the Art. 29 Working Group's (WP29) **Draft Guidelines on Consent** under Regulation 2016/679 (WP 259). We believe that more cooperation and exchange between data protection authorities and practitioners is needed to translate the legal text of the GDPR into practice and reduce legal uncertainty.

In our working group on data protection we gather more than 600 data protection professionals, most of which most practicing data protection officers, who are currently commonly working on the interpretation and application of the GDPR. Furthermore, Bitkom has dedicated considerable efforts in the implementation phase. We have published several practical guidelines for companies. In this process we have identified a number of concrete, practical issues which we would be happy to highlight and thereby contribute to the work of the WP29 with regard to these Guidelines on consent under the GDPR.

In addition to many other provisions of the GDPR, the definition of consent in Article 4(11) of the GDPR comes into effect on 25th of May 2018. The definition and scope of the concept of consent as one of the legal ground for processing if of the utmost importance - not only for the digital economy but also for all other sectors.

When interpreting and applying the GDPR, the importance of consent as one of the legal grounds for processing cannot be underrated. The practical implementation of conditions for a valid consent, the openness and appropriateness for new and emerging technologies should be considered. This said, due to the high requirements formulated by the WP29, the current Draft Guidelines leave little room for a practical, viable implementation of techniques to obtain a valid consent. Furthermore, the Draft Guidelines all but remove the basis for further processing from the scope of the GDPR, which we assume was not the intention.

There are also several point in which the WP29 apply a higher standard that provided

Federal Association
for Information Technology,
Telecommunications and
New Media

Susanne Dehmel
Managing Director
Law and Security
P +49 30 27576 -223
s.dehmel@bitkom.org

Rebekka Weiß, LL.M.
Data Protection &
Consumer Law
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

for in the GDPR and therefore exceed the legal requirements. This should be amended so the Draft Guidelines reflect the provisions rather than going beyond what is legally requested of controllers. Furthermore, the Draft Guidelines contain multiple "Best Practice" examples. In this regard, we ask the WP29 to clarify that some of the criteria and measures set out in these examples or going beyond the legal requirements and are neither compulsory nor introduce a new standard of interpretation of the GDPR.

The aim of this position paper is to draw attention to the difficulties in interpreting and implementing the law.

2. Specific Aspects of the Draft Guidelines

2.1. Definition:

Art. 4(11) of the GDPR defines *"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 conditions of this concept already exceed the previous definition of the Data Protection Directive and hence should not be widened further without indication in the provisions of the GDPR.

2.2. Consent and Imbalance of Power:

2.2.1. Employment

The conditions laid down by the Draft Guidelines for consent in the employment context (page 8) are far too narrow. The Draft Guidelines falsely argue that an imbalance of power is a given fact in the employment context. The WP29 furthermore state that only in exceptional circumstances consent can be freely given. We strongly disagree with this assessment. Firstly, the Guidelines should clarify that the employment context can be a situation of imbalance. Secondly, limiting consent to exceptional circumstances is too narrow and do not sufficiently consider the aspects of each individual case. The GDPR also does not place such a strict burden on controllers. Recital 43 clarifies that consent should be *freely given and it should not provide a legal ground for 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.* This Recital clearly shows that the employment context does not constitute an imbalanced situation per se.

2.2.2. "Compulsion"

The Draft Guidelines also address cases of "compulsion", however, the GDPR does not provide for such a case. It is therefore unclear which cases are affected by this and what exactly "compulsion" means in the context of consent. We urge the WP29 to clarify whether the concept of compulsion derives from the employment context and would like to encourage further discussion on that point.

3. Conditionality:

The Draft Guidelines state that the two lawful bases for processing of personal data, i.e. consent and contract cannot be merged and blurred (page 9). The meaning and scope of this interpretation is unclear and exceeds the provisions of the GDPR. The Guidelines should clarify that the GDPR allows for the controller to decide on one legal ground for one processing purpose and another legal ground for a different one.

The Draft Guidelines state that there are some cases where conditionality would not render the consent invalid (page 10). WP29 should clarify that where the processing is necessary to provide a service, "tying" the provision of a service to a request for consent to process personal data would be permissible. For example, for special categories of data, where performance of contract/provision of service is not an appropriate legal basis, the processing may still be necessary to provide a service. In such a case, the controller would need to make the explicit consent conditional on the provision of the service.

Regarding the provision of free services it is also important to clarify whether the Draft Guidelines take the view that consumers have a right to get access to a service regardless whether they consent to the processing of data by the controller and provider of a (free) service. In our view, this view would exceed the GDPR´s rules. We strongly urge the WP29 to not broaden the concept of Art. 7(4) and Recital 43 of the GDPR in this matter. This would effectively end free online content.

Also, the Draft Guidelines should include examples of where consent would be valid and a lawful ground for processing. Furthermore, we ask the WP29 to clarify that consent would also be valid if the data subject obtains a benefit (f.i. signing up for the newsletter of a company would grant the data subject a discounted price).

4. Granularity:

The Draft Guidelines suggest that a controller seeking consent to multiple purposes of processing should provide a separate opt-in for each purpose. But Article 6 allows for consent to processing for "*one or more specific purposes*" indicating that consent can be obtained for multiple specific purposes. Where purposes are related, conceptually similar, or technically dependent on each other, it will be clearer, more informative, and more sensible for the data subject to provide/revoke consent to those multiple purposes together.

5. Detriment:

Page 8 of the Draft Guidelines states that consent may not be considered to be freely given where there are "significant negative consequences (e.g. substantial extra costs)" if the data subject does not consent. This suggests that some negative consequence or some extra cost wouldn't amount to the level of a detriment. However, on page

10, the Draft Guidelines ratchets the standard to an unrealistic level by requiring that controllers build two "genuinely equivalent" services ("including no further costs")-- one that includes consenting to the use of personal data for additional purposes and an equivalent service that does not involve consenting to data use for additional purposes. This standard is repeated on page 11 ("the controller needs to prove that withdrawing consent does not lead to any costs for the data subject").

The WP29 therefore states that the controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment and bases that statement on Recital 42. The WP29 also states that the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and thus no clear disadvantage for those withdrawing consent. The Draft Guidelines also include the opinion that if a controller is able to show that a service includes the possibility to withdraw consent without any negative consequences e.g. without the performance of the service being downgraded to the detriment of the user, this may serve to show that the consent was given freely. But Recital 42 only provides that the controller, where processing is based on the data subject's consent, should be able to demonstrate that the data subject has given consent to the processing operation. It does not include a further responsibility to demonstrate or prove the possibility to withdraw consent without negative consequences.

This is problematic and should be amended because funding via advertising is not unique to the online environment, and the WP's impractical standard would threaten the livelihoods of publishers, content providers, and service providers that are able to provide their content or service for free because it is ad-supported. Some kind of subscription fee would be required to support businesses in the absence of ads (or certain types of ads). This would dramatically reduce publisher revenue, which has relied on advertising to a far greater extent than subscriptions for a very long time. Many studies show that only a very small portion of users are willing to pay for, e.g., news content.

Similarly, some data processing enables additional functionality or features, so the data subject can freely choose not to turn on the additional functionality or features that requires such data processing, but the experience may appear "downgraded." WP29 should clarify that consent may still be valid even where there is some cost or trade-off in functionality, but that the controller may not impose excessive costs out of proportion with the service or substantially degrade functionality unnecessarily.

6. Specific:

On page 12, the WP29 sets out requirements on the specificity of consent. In point ii) the WP29 states that separate opt-ins are needed for each purpose. We disagree with this assessment as the GDPR does not provide for such a requirement once the purposes are related. Furthermore, the GDPR does not require an opt-in but an (unambiguous) indication of the data subject´s will to consent. We would ask the WP29 to amend the Draft Guidelines in this regard to reflect the language used in the GDPR. This would serve to avoid uncertainty. As the phrase "opt-in" is not used in the legal text of the GDPR, the Draft Guidelines should also maintain the legal wording.

7. Informed

7.1. Multiple (Joint) Controllers

WP29's Draft Guidelines acknowledge that clear, concise, and plain language is important for informed consent, and that layered information can be an appropriate way to be both precise and understandable, especially to accommodate for small screens or situations with restricted room for information. We support this assessment.

However, the Draft Guidelines also state that in the case of multiple joint controllers, "these organisations should all be named." A long list of corporate entity names would not be particularly informative to a data subject (and would take crucial attention away from other key aspects of the consent, like the purpose of the processing). WP29 should clarify that information about co-controllers should be presented in plain and simple language and in a manner that appropriately informs the data subject (e.g., with a secondary layer including additional detail or examples).

7.2. Processors

The Draft Guidelines also address Art. 13 und 14 GDPR with regard to the obligation to provide information on the recipients or categories of recipients including processors. The WP´s view on the question whether it is sufficient to provide a list of categories of recipients is clarified in the Draft Guidelines on transparency (page 32: "In accordance with the principle of fairness, the default position is that a data controller should provide information on the actual (named) recipient of the personal data. Where a data controller opts only to provide the categories of recipient, the data controller must be able to demonstrate why it is fair for it to take this approach."). We do not support this assessment, because neither Art.13 or 14 nor the provisions on fairness support this view.

Also, in the interests of practicality (especially in the context of the change of controller-processor relationships), we suggest amending the Draft Guidelines to an interpretation that naming the categories of recipients is sufficient. This view is also supported by the wording of Article 13(1) lit.3 and Article 14(1) lit.3 of the GDPR, since the information about categories of recipients is described as an alternative to the specific name of the recipient. This is actually also supported by considerations with regard to business and trade secrets and for IT and data security reasons (e. g. naming the concrete storage locations of the data could trigger a security risk).

7.3. Declaration of Consent

On page 14 the WP29 argue that the declaration of consent must be named as such. The wording "*I know that…*" is considered as not meeting the requirements of clear language. We strongly disagree with this assessment, as the GDPR does not provide for such a strict interpretation and wording such as „*I know that*" sufficiently shows the data subject that he is consenting to something (a processing).

7.4. How to Provide Information

We welcome the WP´s clarification that a valid and informed consent is also considered to be given when not all the information set out in of Article 13 and Article 14 of the GDPR are given during the process of obtaining consent.

8. Audience

The WP29 states that a controller must assess what kind of audience it is that provides personal data to their organization. This general requirement goes beyond the requirements of the GDPR. The Draft Guidelines should therefore be amended in this regard.

9. Unambiguous

While Recital 32 is clear that silence, pre-ticked boxes, or inactivity do not alone constitute consent, the text of the GDPR still allows controllers to abide by principles of privacy by design to establish appropriate defaults for data collection and processing. The Draft Guidelines go beyond that which is supported by the text of the GDPR to state "the use of pre-ticked opt-in boxes is invalid under the GDPR" (page 16) and "the GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement" (page 17). A controller should be able to offer default options that require the data subject to either affirmatively indicate agreement or to decline or modify the option. Requiring that all data collection and processing options be default-off across all services would increase click fatigue, impair user experience and service functionality, and limit controllers' design freedom.

WP29 should clarify that pre-ticked opt-in boxes won't alone constitute consent, but that where the consent requirements are otherwise met (e.g., by the inclusion of a separate mechanism to indicate agreement), an appropriate default may be used.

10. Preventing Click Fatigue

The WP states that it is the controller´s obligation to prevent consent fatigue. This requirement is very onerous for controllers and requires a difficult assessment, given the uncertainty. Best practice should, instead, be envisaged as an open and ongoing dialogue with the parties involved (controllers, regulators, other stakeholders) so that the responsibility for managing consent is shared and can evolve in a flexible way with the technology. Suggestions to prevent consent fatigue could include relying on alternative legal bases for processing wherever possible, using clear and plain language and layered information, and allowing consent to multiple purposes whenever it would be appropriate to do so (e.g., if they are similar, related, or dependent on one another).

11. Explicit Consent

The Draft Guidelines describe a standard for explicit consent that is not supported by the text of the GDPR and that would be unworkable for many controllers. For example, requiring that a data subject fill in a form, send an email, upload a scanned document, or use an electronic signature would require the data subject to provide additional

personal information that they otherwise would not have needed to do and takes the user out of the context of the service.

The WP29 should adopt a standard whereby "an explicit consent statement" (e.g., "I consent to [processing]") is presented to the data subject that the data subject could accept by clicking a button, ticking a box, or turning on a setting. This standard was also described by the ICO in its guidance on consent under the GDPR.

12. Interaction between Consent and other Lawful Grounds

The WP29 outlines on page 12 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". Furthermore, the Draft Guidelines state that "as a general rule, a processing activity for one specific purpose cannot be based on multiple lawful bases" (page 22) and "under the GDPR, controllers that ask for a data subject's consent to the use of personal data shall in principle not be able to rely on the other lawful bases in Article 6 as a 'back-up'" (page 22). However, this interpretation is contra legem as Article 6 states that processing is lawful when "*at least one*" of the legal bases applies, clearly indicating that multiple legal bases may apply. Also, on page 30, the WP29 states that under the GDPR it is not possible to swap between one lawful basis to another.

Pursuant 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 bases the controller must apply a compatibility test in compliance with Art. 6(4) GDPR. Recital 50 also 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. Accordingly, pursuant to Article 6(4) of GDPR, the controller may process data for compatible purpose without seeking a new consent. Therefore 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 regard to the WP29 statement that "As a general rule, a processing activity for one specific purpose cannot be based on multiple lawful bases" we would also like to make some remarks. We assume that the WP29´s intention what not to suggest that if a consent proves to be invalid, the controller could not change to another legal basis.

The following reasons speak against the abovementioned interpretation of the relationship between the conditions of legality:

- The clear wording of Article 6(1) of the GDPR stipulates that processing is lawful if at least one of the following conditions is met. It follows from the wording that processing of personal data can be based on several bases simultaneously.
- This interpretation is also supported by Art. 17(1)(b) of the GDPR, which stipulates that an obligation to delete data only exists if consent is revoked and there is no other legal basis for processing.
- The transparency obligations and information requirements are already adequate protective measures for the data subject – there is not objective reason for such a restrictive interpretation and the contra-legem reduction of the processing possibilities under the GDPR.
- This is also provided for in Recital 50 of the GDPR, which states that the processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required.

As processing for compatible purposes and the use of multiple legal bases is explicitly provided for in the GDPR, the WP29 has no foundation to now suspend it. We ask the WP29 should clarify that controllers may rely on multiple or alternative legal bases for processing and on compatible purposes for processing.

13. "Expiration" of Consent Given for Children

The Draft Guidelines state that "consent by a holder of parental responsibility or authorized by a holder of parental responsibility for the processing of personal data of children will expire once the data subject reaches the age of digital consent" and "in practice this may mean that a controller relying upon consent from its users may need to send out messages to users periodically to remind them that consent for children will expire once they turn 16 and must be reaffirmed by the data subject personally" (page 25). This assessment is not supported by the GDPR as the GDPR does not provide for a requirement to obtain consent again after the data subject reaches the age of digital consent. It would also be impractical to remind the users regularly about such a requirement as this would lead to consent and information fatigue.

Whereas it is clear that from the day the data subject reaches the age of consent, the controller needs to obtain any new or additional consent from the data subject herself, the guidelines should be clarified so it is also clear that the consent previously given by the parent allows the provider to continue the processing of personal data. Children could be notified that they can exercise their rights on their own (which would obviously include revocation of consent), and should be given the means to take control of their personal data/the service that is being provided to them. Also, any processing operations that were not covered by the consent previously provided by the parent would require additional consent.

However, children should not be obliged to provide consent on their own if they do not want to. Obliging children to take control of their personal data/the service that is being provided to them without the alternative of continuing to operate under their parents' consent would not give them free choice. The relevant point here is that the data subject needs to be clearly informed of the possibility to take control over her personal data, and that she is given the necessary means to make the choice between taking control of her personal data/the service that is being provided to her, or remain under her parents' consent. If children are notified by the controller that they can take control of their personal data and how they can do that, but decide not to do it, then it would be reasonable for the controller to continue providing the service and processing the personal data under the consent provided by the parent, which is reaffirmed by the data subject herself by taking the decision to remain under their parents' consent.

14. Provision of Information to Children

Furthermore, with regard to the provision of information to children, the WP29 establishes that "in order to obtain "informed consent" from a child the controller must explain in language that is clear and plain for children how it intends to process the data it collects. Since consent can only be obtained from the child herself when she is above the age of consent, it seems that the WP29 intends to establish that individuals above the age of consent must be provided with child-centred information, which is also their position in its Guidelines on transparency. From Bitkom's perspective, it is unclear how this is to be understood.

14.1. Definition of "Children"

The definition of "children" for general legal purposes is provided by international instruments and national laws. However, GDPR clearly establishes the threshold for the application of data protection obligations with regard to children: data subjects under 16, unless Member States decide to set a lower age provided that such lower age is not below 13 years. There is no support under GDPR to determine that individuals above the age of consent in the respective country need to be provided with child-centred information. Establishing that such an obligation arises from Recitals 38 and 58 of GDPR would be factually and legally incorrect.

It is clear that Article 8 of GDPR establishes the obligation to obtain parental authorisation for the processing of children's data based on consent when children are below the age of consent. It is also clear that Recitals 38 and 58 do not mention that controllers are obliged to provide child-centred information to users above the age of consent. If GDPR had intended to impose the obligation to provide child-centred information to users above the age of consent and, therefore, to impose a different threshold than that established by Article 8, it seems reasonable to think that GDPR would have made that clear in the Recitals and that the obligation would be set out in at least one of its 99 articles (as the obligation to obtain parental consent is established in Article 8).

However, that is not the case. Apart from the above, it's not clear how the obligation to provide child-centred information to individuals above the age of consent would be more beneficial for the data subject. Taking the

example of child-centred language included by the Working Party in its guidelines, it is difficult to understand how the UN Convention on the Rights of the Child in Child Friendly Language would be appropriate for a 17 year-old data subject, for example, when the same data subject is obliged to read Jane Austen or Shakespeare at school. This conclusion is even more obvious when considering that, nowadays, children are digital natives (i.e., more likely to understand some data processing terms even better than many adults). Providing child-centred information to individuals above the age of consent could have a counter-effect, as it would be below their level of understanding and maturity. Such child-directed text would be less likely to resonate with them, and they would be less willing to engage with the message.

14.2. Interpretation of "Offered Directly to a Child"

The Working Party mentions that "if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (...) then the service will not be considered to be 'offered directly to a child' (...)". However, as mentioned above, even if the definition of "children" for general legal purposes is provided by international instruments and national laws, GDPR clearly establishes the threshold for the application of data protection obligations with regard to children: data subjects under 16, unless Member States decide to set a lower age provided that such lower age is not below 13 years. There is no legal support under GDPR to refer to the age of 18 in the guidelines.

Therefore, the reference to 18 should be changed to a reference to the relevant age of consent in the specific country. Also, the guidelines should clarify that the possibility of service providers to indicate that their service is only offered to users above the age of consent is just one of the ways to determine that the service is not offered directly to children (not the only way). In particular, only services that are primarily targeted to children below the age of consent based on their content and features should be considered "directly offered to children" for GDPR purposes, and the service provider should not need to expressly clarify what their targeted audience is.

14.3. Age Verification

The Working Party establishes that "when providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent" and that "if the users state that they are over the age of digital consent then the controller can carry out appropriate checks to verify that this statement is true. Although the need to verify age is not explicit in the GDPR it is implicitly required, for if a child gives consent while not old enough to provide valid consent on their own behalf, then this will render the processing of data unlawful".

The need to verify age is neither explicit nor implicit in the GDPR. Quite the opposite: GDPR itself expressly requires personal data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Article 5). GDPR also foresees that "if the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to

maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation" (Article 11). An obligation for controllers to verify age would require them to process extensive personal data. Establishing real-world identity is very challenging in practice and would imply processing a significant amount of data. This could be disproportionate and could become a barrier to access to everyday services that could risk creating digital exclusion. In addition, even if this was undertaken, it's not clear whether the result would be reliable enough in all cases.

14.4. Children's Consent and Parental Responsibility

As a general comment in relation to verification of parental consent mechanisms, we welcome the Working Party's recommendation for a reasonable and proportionate approach. Parental consent mechanisms should not lead to excessive data collection and controllers should have sufficient flexibility to implement different kinds of mechanisms and make them evolve as technology advances.

With regard to the verification through bank details (one of the examples set out by the WP29 when referring to verification of parental consent mechanisms that are suitable for high-risk cases), the guidelines should specify that providers could charge a small amount if they need to, but the collection of the credit/debit card details without charging any amount should be sufficient to verify parental consent as it would meet the same purpose (verifying that the card is real and active). Charging an amount of money does not make the verification method any more robust, and could be a barrier for users to access digital services. For example, parents may be reluctant to provide their card details because they may not understand why a service that is supposed to be provided for free needs to make a charge. Other parents could consider the charge as discriminatory in cases where they don't have the funds to cover even a small charge (e.g., delinquent accounts) or don't have the means to have a credit/debit card. In other situations, small charges could be suspicious of fraudulent activity and banks could block them before they are processed.

The guidelines also mention that "in low-risk cases, verification of parental responsibility via email may be sufficient". However, it's not clear what situations should be categorized as "low-risk cases" and why verification via email should only apply in those situations. There is no legal support to defend that verification via email or via the parent's password (when the parent has an existing account with the service provider) could not be a robust mechanism for both low and high risk situations. This is especially the case when this mechanism is combined with other information that the provider may have that may lead to believe that the email/account holder is an adult, and when this method is combined with further action by the provider if there are any complaints.

In relation to the above, it should be noted that, as recognized by the Working Party, Article 8 of GDPR requires controllers to make reasonable efforts to verify parental consent and this applies to both low and high-risk scenarios. It is also worth pointing out that, based on research, many parents are generally reluctant to provide credit/debit card details because they consider it too intrusive. Therefore, other mechanisms should be a possibility for service

providers in all types of risk situations, and authorities should encourage them in order to promote the implementation in practice of the verification of parental consent obligation.