Position Paper

Bitkom views on Article 29 Working Party Draft Guidelines on Transparency 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 Transparency** under Regulation 2016/679 (WP 260). 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, of which most are 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.

We appreciate the recommendations of the WP29 on how to implement the GDPR´s principle of transparency into practice. However, some of the interpretations of the WP29 seem overly restrictive and go beyond what is required by the GDPR. Bitkom is convinced that the legislator has provided a comprehensive set of rules to ensure full transparency on the processing of personal data to the data subject. It should be reconsidered if it is appropriate and necessary to go beyond the transparency obligations set by the GDPR and introducing further obligations derived from principles like fairness or best practice. Bitkom also questions whether these further obligations will improve transparency to the data subject. The WP29 should therefore not introduce unwritten transparency obligations as this will lead to uncertainty amongst controllers and data subjects alike.

The aim of this position paper is to draw attention to the difficulties in interpreting and implementing the law and show the need for a clarification regarding the discretion on how to deliver transparency.

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

2. Specific Aspects of the Draft Guidelines

2.1. Best Practice Example on Consequences (page 8, no° 9)

The Draft Guidelines state that the data subject should be able to determine in advance what the scope and consequences of the processing entail. As a best practice, the WP29 suggests, in particular for complex, technical or unexpected data processing, controllers should not only provide the prescribed information under Articles 13 and 14, but also separately spell out in unambiguous language what the most important consequences of the processing will be. As this example has no basis in the GDPR, this point should be reconsidered. In Bitkom´s view, it is also unclear about what consequences the data subject should be informed.

It would also be challenging for controllers to provide information to data subjects about "unexpected" processing without being speculative about how data subjects may react to it and potentially raising unnecessary alarm. We would also like the WP29 to clarify what is meant by "most important consequence". Additional requirements should not be introduced in this regard, especially because it is questionable whether additional measures would lead to more transparency. The requirements set out in Art. 13 and 14 are already high, it would unduly burden controllers if more obligations were to be introduced here.

2.2. Easily Accessible (page 8, no° 10)

The WP29 states that the "easily accessible" element means that the data subject should not have to seek out the information; it should be immediately apparent to them where this information can be accessed, for example by providing it directly to them, by linking, by clearly signposting it or as an answer to a natural language question.

According to the examples for "easily accessible" "once an app is installed, the information should never be more than "two taps away". Generally speaking, this means that the menu functionality often used in apps should always include a "Privacy"/ "Data Protection" option." This requirement would hamper the usability intensely, since in every submenu the respective link to the data privacy information must be implemented. This contradicts the logic of layered information. Therefore it should be sufficient if data privacy information is accessible via two clicks from the (app's) starting page.

2.3. Clear and Plain Language (page 9, no° 11)

The WP29 states that with written information (and where written information is delivered orally, or by audio/audiovisual methods, including for vision-impaired data subjects), best practices for clear writing should be followed. The Draft Guidelines therefore states that the requirement for clear and plain language means that information should be provided in as simple a manner as possible, avoiding complex sentence and language structures. The information should be concrete and definitive; it should not be phrased in abstract or ambivalent

terms or leave room for different interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear.

The Guidance sets an unreasonable standard in terms of specificity for controllers with multiple products and more complex services and invites "notice fatigue" for data subjects. Controllers should be able to meet the "clear" language bar through a combination of explaining the purpose in "plain" language and then providing specific examples of the type of processing that fits under that description.

The Guidance states that controllers may not use phrases such as:

- "We may use your personal data to develop new services' (as it is unclear what the services are or how the data will help develop them)"
- "We may use your personal data to offer personalised services' (as it is unclear what the personalisation entails)"

Requiring controllers to detail, for example, each type of new service that may be developed places an impracticable burden on controllers and conflicts with the transparency principle of promoting user comprehension, as the practice would result in too detailed notices.

In the case of user research, it is impracticable for a controller to provide specific detail on research projects given the nature of that processing pertains to experimentation and development that is inherently not clearly defined.

We therefore strongly disagree with these arguments set out in the Draft Guidelines regarding °no 11. The information about the use of data to improve products and services is transparent and not unclear. Furthermore, it is the common practice to inform users in this way and there is no evidence that data subjects do not understand such information. Reasons of business confidentiality would also make it difficult for controllers to inform about every concrete development process regarding improvements of their products. As improvement processes develop over time, it may be nearly impossible to give precise and detailed information on the processes. However, we agree that information on changing purposes is necessary, where the GDPR requires it.

2.4. Transparency Obligations Regarding Children (page 10, no° 13)

In interpreting the scope of transparency obligations for children, the WP29 states that this obligation applies when: controllers are targeting children or are (or should be) aware that their services are particularly used by children. There is no textual support under the GDPR which would require controllers to assess the age of the audience that is providing personal data to their organization to determine whether their services are being used by children. Rather, the GDPR requires that controllers minimize their processing of data to what is necessary: personal data must be

"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Article 5).

Further, the GDPR states 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 identify their audience would require them to process extensive personal data in violation of Article 11. To provide controllers with more certainty about the applicable standard, while also implementing a proportionate solution, we should look to the applicable test under the Children's Online Privacy Protection Act (COPPA) for when obligations apply -- either when a service is directed to children or the provider has "actual knowledge" that they are collecting personal information from a child.

The Working Party refers to "children" as "individuals of 16 years or older (or, where in accordance with Article 8.1 of the GDPR Member State national law has set the age of consent at a specific age between 13 and 16 years for children to consent to an offer for the provision of information society services, children who meet that national age of consent)", and establishes that the obligation to provide information in "child-centred language" applies when children are within that age-range. 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 is 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 children above the age of consent.

If GDPR had intended to impose the obligation to provide child-centred information to children above the age of consent and, therefore, to impose a different threshold than that established by Article 8, the Regulation would have made that clear in the Recitals and set out the obligation in at least one of its 99 articles (just as the obligation to obtain parental consent is established in Article 8). However, that is not the case.

Apart from the above, and from a practical point of view, 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, especially when the Regulation establishes a clear rule that these individuals are sufficiently mature to make their own consent decisions about data processing.

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. Children above the age of consent are already mature enough to understand general audience texts. This conclusion is even more obvious when considering that, nowadays, children are digital natives (i.e., more likely to understand data processing terms than many adults).

Providing child-centred information to children above the age of consent could have a counter-effect, as it would be below their level of understanding and maturity. Such a text would be less likely to resonate with them, and they would be less willing to engage with the message (i.e., a plain text accompanied by cartoons, such as that offered by the UN Convention on the Rights of the Child in Child Friendly Language, may be appropriate for a younger child but is likely to be ignored by an older data subject).

With regard to the requirements of transparency regarding children it is important to notice that the GDPR did not implement a fully harmonized minimum age throughout the European Union. This leaves controllers already in a difficult situation when they want to process data from different countries in the EU. Against this background, no additional requirements should be introduced here. The provisions of the GDPR guarantee a sufficiently high protection level.

2.5. Method of Information (page 11, no° 15)

Method of information depends on the circumstances in which controllers and data subjects interact (appropriate measures). In Bitkom´s view, the different distribution channels are not sufficiently taken into account here. „Appropriate" refers to a necessary balance between the interest of the concerned data subjects in information and the effort the provider is reasonably able to make. Therefore, there cannot be a "one-fits-all-rule"; instead, it is essential to take the specifics of the relevant use cases (e.g. online channels, call centre, shops) into account and to leave room for necessary adaptions on a case-by-case basis.

Different mechanisms for the different use cases must be accepted. E.g. if the user books a product on a webpage it must be sufficient to prominently display a link to the relevant data privacy information on the page. If the user orders a product via a telephone hotline it must be sufficient to explain to him where he can find the data privacy information - as it will not be possible to read the data privacy information to him while he is on the line. With regard to the right of access (Art. 15) it should be clarified that if data subjects use a customer service platform, it should be sufficient to refer data subjects to the platform, if a process for gaining access is implemented on the platform.

We would like the WP29 to clarify and redefine this aspect of the Draft Guidelines.

2.6. Oral Provision of Information (page 11, no° 17)

If the data subject requests the information orally, the provider should "allow the data subject to re-listen to pre-recorded messages. This is imperative where the request for oral info relates to visually impaired data subjects or other data subjects who may have difficulty in accessing or understanding info in written format". The controller must document ("has a record of") (i) the request for information by the person concerned in medium form, (ii) the method of verification of the person concerned (if necessary, cf. above) and (iii) the fact that the information has been transported to the person concerned. This goes beyond the provisions of the GDPR and therefore extends the scope of the relevant requirements. It is necessary to leave it to the controllers to decide on how to fulfill the requirements. Furthermore, we would like the WP29 to clarify that the suggestions made in this regard are not binding new requirements.

2.7. Details of Article 13 and 14 of the GDPR (page 12 ff)

The Guidelines go beyond the text of Articles 13 and 14 to specify particular detail that controllers must provide to data subjects, which places a disproportionate burden on complex organizations without a resulting gain to users in terms of the value of the information provided.

For example:

- If a controller is using legitimate interest as its basis for processing, the Guidance says it should inform the data subject of the particular interest and provide information from the balancing test. The statement that controllers need to provide information on the balancing test goes beyond the text of the Regulation and poses a risk to proprietary decision-making, as well as presents concerns about notice fatigue.

- Article 13 reasonably allows controllers to identify the “categories of recipients” of data. Providing granular detail like the industry, sector and sub-sector, and location of these recipients is overly burdensome and likely to overwhelm data subjects with detail.

- There is no basis under Article 13 to require controllers to identify each third country to whom data is transferred, and the value of this information to the data subject is not clear.

- According to the wording of the GDPR controllers should be able to satisfy Article 13.2(b) and Article 14.2(c) by informing the data subjects about the existence of the of the tools available.

- Furthermore, the Draft Guidelines state that controllers need to inform users about the specifics of where they’re entitled to make complaints. This goes beyond the text of Article 13 and 14 of the GDPR.

- The Draft Guidelines state in paragraph 19 that there's no difference between the status of the information to be provided under sub-article 1 and 2 of Articles 13 and 14. This is not supported by the text of the Regulation. Subarticle 2 of Articles 13 and 14 both contain the caveat that the data subject should be provided with further information "necessary to ensure fair and transparent processing," which is not contained in Subarticle 1. To give meaning to that phrase, it must be the case that controllers have more flexibility to provide the information in Subarticle 2 based on an assessment of where it's necessary for fairness reasons. That may mean that the information is not provided in the same place as the requirements in Subarticle 1.

2.8. Accountability with Regard to Transparency (page 13, no° 22)

Given concerns about information fatigue, it should be reasonable for controllers who are making non-material updates to their Privacy Notices to provide notice within the Policy itself. The Guidelines make the blanket statement that "[r]eferences in the privacy statement/ notice to the effect that the data subject should regularly check the privacy statement/notice for changes or updates are considered not only insufficient but also unfair in the context of Article 5.1(a),". We strongly disagree with this assessment.

If controllers do not tailor their form of notice to the user based on the impact of the changes they're making, then there's significant potential for user confusion, especially where many controllers are making non-material updates in advance of the GDPR implementation deadline. It is in the data subjects own interest to have control over their own data. Such control presumes gaining information about processing with regard to personal data. It is reasonable and not "unfair" to ask data subjects to also look at privacy policies, with the understanding that controllers are responsible for providing data subjects with notice about material changes.

2.9. Regular Re-acquainting (page 16, no° 28)

The Draft Guidelines state that controllers should regularly draw the attention of the data subjects to the privacy notice once again. This goes beyond the legal requirements and we ask the WP29 to adjust the Draft Guidelines in this regard.

2.10. Other Types of appropriate measures (page 18, no° 33)

In general, the information requirements can be fulfilled when using an electronic privacy statement/notice. But the Draft Guidelines set out examples where different/additional measures may be required depending on the contact situation. We would also like clarification with regard to the given examples, e.g. whether the additional information would be needed in the telephonic environment, as we see no such requirement in the GDPR.

While we welcome that the WP29 gives examples on this issue, the given situations are too specific in our opinion. They should be more generic to accommodate for a broader set of cases.

2.11. Information on Profiling and Automated Decision-Making (page 19, no° 34)

Regarding the provision of information about the logic involved in automated decision-making, the WP29 should include clarification that the information requirements still provide protections for controllers to not disclose proprietary information.

Furthermore, automated decisions with a merely positive effect should be subject to a less strict regime in terms of transparency requirements, in particular, in relation to the requirement to provide meaningful information about the logic involved, the significance and the envisaged consequences of the automated decisions. In this regard we refer to our position paper for the WP´s Draft Guidelines on automated individual decision-making including profiling.

2.12. Visualisation Tools (page 21, no° 42)

According to the WP29, Recital 58 indicates that the accessibility of information addressed to the public or to data subjects is especially important in the online environment. We do not agree with this general understanding of Recital 58 that accessibility is especially relevant with regard to the online environment. Recital 58 states 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 and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."* The Recital therefore does not concern accessibility of information in the online environment per se.

Furthermore, the WP29 states in the corresponding footnote 36: "in this context, controllers should take into account visually impaired data subjects (e.g. red-green colour blindness)". While we agree that it is important to enable visually impaired data subjects to read and receive the necessary information, the statement of the WP29 is beyond the scope of Recital 58 and the issue of visualization as this should primarily deal with visualization tools such as icons, certification mechanisms, and data protection seals and marks).

2.13. Exercise of Data Subject´s Rights (page 23, no° 48)

The WP29 states that the modality provided by a data controller for data subjects to exercise their rights should be appropriate to the context and the nature of the relationship and interactions between the controller and a data subject. To this end, a data controller may wish to provide different modalities for the exercise of rights which are reflective of the different ways in which data subjects interact with that data controller.

We are not certain, what exactly this entails and would like clarification on this point. Regarding the given examples we would also like to voice concern and would like clarification why the WP29 does not support a practice where the

data subject has to contact the customer service department. Especially with regard to health data it seems to be the more prudent way of providing information and enabling interaction if the identity of the data subject can be checked before sending him (confidential) health data or other related information. We would therefore not deem this practice example as "poor".

2.14. Proves Impossible (page 26, no° 52)

The situation where it "proves impossible" under Article 14.5(b) to provide the information is an all or nothing situation because something is either impossible or it is not, according to the WP29. While we agree that there are no "degrees of impossibility", we would like clarification that each individual case has to be assessed separately. Also, the GDPR also included situations where complying with the transparency obligations would involve disproportionate efforts.

Furthermore, the WP29 argues that "if a data controller seeks to rely on this exemption it must demonstrate the factors that actually prevent it from providing the information in question to data subjects. If, after a certain period of time, the factors that caused the "impossibility" no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so. In practice, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects".

In our view, it is still unclear how the controller would become aware of the changed situations, because if it was previously impossible to provide information to the data subject, and the circumstances change, when and how does the controller become "aware" that transparency efforts are now possible and can be complied with? We would like the WP29 to issue guidance on this question.

2.15. Schedule (page 31-35)

With regard to the schedule we would like to voice our concern that the WP29´s interpretation often go beyond the legal requirements of the GDPR and do not provide specific and clear guidance on what information has to be given in the data protection notices. We ask the WP29 to issue more guidance in this regard, clarify the given examples and to not extend the scope of the GDPR´s provisions.

In this regard, we would like to specify our concerns with some of the aspects in the schedule (no exhaustive list):

- **Art. 13.1 (c):** *"In addition to setting out the purposes of the processing for which the personal data is intended, the relevant legal basis relied upon under Article 6 or Article 9 must be specified."*

  We are not certain, how far this requirement to specify the relevant legal basis goes. We would like clarification on this point and especially whether it would be sufficient to provide the abstract legal basis. It should be necessary to enumerate the legal basis in the data protection notices and give this information at the beginning of the data protection notices.

- **Art. 13.1 (d):** *"The specific interest in question must be identified for the benefit of the data subject. As a matter of best practice, the data controller should also provide the data subject with the information from the balancing test, which should have been carried out by the data controller to allow reliance on Article 6.1(f) as a lawful basis for processing, in advance of any collection of data subjects' personal data."*

  This requirement goes beyond the GDPR´s provisions and should therefore be amended. The GDPR does not include an obligation to provide information on the balancing test.

- **Art. 13.1. (e):** *"The term "recipient" is defined in Article 4.9 such that a recipient does not have to be a third party. Therefore, data controllers, joint controllers and processors to whom data is transferred or disclosed are covered by the term "recipient" and information on such recipients should be provided in addition to information on third party recipients. In accordance with the principle of fairness, the default position is that a data controller should provide information on the actual (named) recipients of the personal data. Where a data controller opts only to provide the categories of recipients, the data controller must be able to demonstrate why it is fair for it to take this approach. In such circumstances, the information on the categories of recipients should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients."*

  We would like to voice concern in this regard. 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 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).

- **Art. 13.1 (f):** *"The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article 45 / binding corporate rules under Article 47/ standard data protection clauses under Article 46.2/ derogations and safeguards under Article 49 etc.) should be specified. Where possible, a link to the mechanism used or information on where and how the relevant document may be accessed or obtained should also be provided. In accordance with the principle of fairness, the information should explicitly mention all third countries to which the data will be transferred."*

  We have a strong concern with this interpretation of Art. 47 GDPR as it seems to be interpreted in a broader way than it actually is. Art. 47 (2) (b) GDPR asks for the identification of the third country or countries, but there is no information requirement in Article 13 GDPR.

- Art. 13.2 (b): *"This information should include a summary of what the right involves and how the data subject can take steps to exercise it. In particular, the right to object to processing must be explicitly brought to the data subject's attention at the latest at the time of first communication with the data subject and must be presented clearly and separately from any other information."*

  There is no requirement in the GDPR to provide information on how the data subject can take steps to exercise his/her rights. This aspect should therefore be amended.