DIGITALEUROPE

DIGITALEUROPE's response to public consultation on Article 29 Working Party draft guidelines on consent under Regulation 2016/679

Brussels, 23 January 2018

INTRODUCTION

DIGITALEUROPE welcomes the opportunity to provide comments on the draft guidelines on consent under Regulation 2016/679 published by Article 29 Working Party (WP29). We were closely engaged in the legislative debate and provided input throughout the process. This involvement provided us with insight into the intentions behind specific provisions. Our members include digital companies with headquarters or significant presence in the EU and European national trade associations, representing large, medium and small companies in the technology sector from across the continent.

While the GDPR has further strengthened alternative grounds for the lawful processing of personal data, it is essential that consent standards remain practical and applicable by all in industry, especially given the disproportionate emphasis that the European Commission's proposal for an ePrivacy Regulation puts on consent. It is therefore important that the standard is not only considered in terms of how it can be practically implemented but that it is also relevant and appropriate to current and emerging technologies, and how a user interfaces with these types of services.

With this in mind, we are concerned that the requirements regarding the lawful capturing of consent specified in the draft guidance document will be so difficult in practice to obtain that they risk removing consent as a viable legal ground on which to process personal data, which we assume is not the intention of the WP29.

DIGITALEUROPE welcomes the emphasis that the WP29 puts on other legal bases and we have consistently advocated for sufficient space for other legal grounds, such as legitimate interest and contract.

The freedom to conduct business, including contractual freedom, is an essential part of how our market-based economy operates and also individual autonomy. It should be up to companies to define the conditions under which they offer their services, the features they integrate and which of these they make optional to their users as well as the most appropriate way to monetize a given service. As long as a company is compliant with the law, can be held accountable, follows a risk based approach, provides transparency and control to its users and integrates privacy in its design process, it should be left to decide how it differentiates itself in a market and what products and features it offers to its users. Indeed, privacy settings and control tools are increasingly becoming market differentiators. Consent or restrictive interpretation of other legal bases should not be used to limit innovation or step into product design and development.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

CONSENT IN ART. 4 (11) OF THE GDPR

The question as to what constitutes affirmative consent is particularly challenging where consent is the only reasonable legal ground and a user is asked to engage on a screen that may be too small, or may not have any interface at all, such as audio-controlled devices.

The draft guidelines, unfortunately, do not address the issue that excessive information simply undermines the very consent it is purporting to collect. It is not a question of seeking to have users consent to uses of their data which are not obvious but rather how to present information in such a manner so a user will, in fact, engage with the notice. The WP29 guidelines fail to discuss this aspect and, therefore, risk causing controllers to overload users with information in the absence of a clear path forward. This would be a bad outcome for users.

FREE/FREELY GIVEN

Not only does the GDPR not refer to "strictly" necessary as a standard, as long as a contract is legal under national law, WP29 should not try to define what is necessary or not to provide a given service. Furthermore, when it comes "tying" a provision of a certain part of a service to consent, this provision should not necessarily or automatically invalidate the consent, especially in cases where the user has been properly and transparently informed and he or she still decided to freely give his/her consent. Once a user has an opportunity to consult the information, which makes clear how the data will be used, and subsequently proceeds to install the app or uses the service, then it is clear that the user is exercising a free choice. There is no detriment, in the legal sense, from the user choosing not to install the app or not to use the service. Users simply do not have to use an app or service, which is available on a commercial basis. It is incorrect to conclude that a user has a choice to use what may be a free service, which by necessity must be monetised in some manner whether by in-app purchases or advertising. The choice of the monetisation method should be left to the controller. In the case of special categories of data, where the contract legal basis is not available, there may also be processing that is necessary to provide a service.

CONDITIONALITY

Whilst the GDPR does make a difference among the legal grounds, i.e. consent and necessary for the performance of a contract, it should be recognised in the guidelines that it also allows a data controller to decide, on one legal ground, for one use of personal data and another more appropriate legal ground for another use or collection. These uses may also arise in the context of the same data collection or in the provision of the same service. In fact, nothing in the text of the GDPR suggests that a processing operation cannot rely on more than one legal basis. Article 6 states that processing is lawful when "at least one" of the legal bases applies - indicating that multiple legal bases may apply. What is required is that a controller be clear to users as to what data it processes, on what basis and why.

Further, the guidelines currently only list examples where consent would not constitute a lawful ground for processing. However, the guidelines concede that there are limited cases where conditionality would not render the consent invalid, and we ask the WP29 to provide some examples of such circumstances.

Finally, we are concerned that the draft guidelines take the view that consumers must receive an equivalent service regardless whether they choose to share data or not. This fails to take account of the

fact that certain services are personalised by their nature, such as a personalised shopping service or a personal music service that must, by necessity, collect personal data to provide the personalised service requested by the user. It is not correct to state that such services cannot be offered on the basis of consent once such a consent otherwise meets the requirements of the GDPR. It is also not correct that the GDPR creates an obligation for a controller offering a personalised service to also offer a non-personalised version. There cannot be an obligation on a controller to invest in offering a service, which they do not believe will provide the high level of satisfaction, which customers seek in a personalised service. There is no obligation to offer such a service under the GDPR. Consent, compliant with the other requirements of the GDPR, would be a valid ground for processing of personal data, once the user subsequently has a right to withdraw from the service with no detriment, such as receiving a refund for a paid service.

DETRIMENT

As mentioned above, it is unrealistic to expect a controller to ensure in all cases that there will be no detrimental impact or consequence for the consumer (i.e. performance of the service being downgraded) if she or he were to withdraw consent. There are a large number of services, which require the use of personal data to provide the service requested by the customer. It cannot be mandated that a controller has to find a way to offer the same service where no such possibility exists. Furthermore, some data processing enables additional functionality or features and the data subject can freely choose not to turn these on. However, the experience may appear "downgraded". Even services with 100% subscriber funded business often rely on upselling from freemium to paid products in order to be financially viable and enable the provision of the free service.

Overall, we strongly argue that the GDPR imposes no obligation on controllers to build two "genuinely equivalent service[s]" and that the WP29 should seek to avoid extending the requirements regarding consent to a level that is impossible for controllers to comply with in practice.

WITHDRAWAL OF CONSENT

In reference to obtaining and withdrawing via one click, it needs to be noted that one click will always only arise after a user is already subscribed to a service. Therefore, for the withdrawal to be effective the user must also be signed in.

It is also necessary to highlight that for reasons of consumer law the implications of losing access to a paid service by the withdrawal of consent need to be made very clear to a user. This is not a matter of making it difficult for users to withdraw consent, but ensuring that all legal rights are adhered to.

Withdrawal should also not trigger automatic deletion or anonymisation as suggested by the WP29. A data subject should be able to choose to withdraw consent going forward and to keep his/her data intact from when she/he had provided consent. As the WP29 noted, data subjects have the separate right to erasure. Thus, and provided there is a prominent means to seek deletion, rather than trigger potentially unexpected and undesired data loss, the controller should await a deletion request from the data subject before taking that action.

The obligation to delete or anonymise data once consent has been withdrawn cannot apply where the personal data is contained within a financial record, which must be retained for financial reporting purposes only, or other instances where the controller may need to retain the data for legal reasons.

IMBALANCE OF POWER

a) Employment

We consider that limiting consent to "exceptional circumstances" alone is too narrow. Consideration as to whether an employee felt under pressure to give consent needs to take account of the precise circumstances that applied. For instance, an offer for employees sent to a large group to participate in a trial of an unreleased product or software completely at their own discretion would not give rise to these concerns. A different situation would apply where a manager approached a specific employee or employees and asked them to participate. An employee participating in such a case would not be considered to be freely doing so. Therefore, we would ask that the WP29 be prepared to provide guidance that is more open in nature and allows for a fuller consideration of all the relevant factors as to whether consent was truly freely given in certain contexts within employment.

b) "Other Situations"

The draft guidelines references cases where there is an element of "compulsion". It is extremely unclear in a commercial context what this actually means in practice and what the WP29 understands as "compulsion". For example, we would question whether cases where social pressure from a circle of friends who are using a service to also join that service so as to be able to communicate with them or play online games, for instance, could be considered to be compulsion. Certainly, in an employment context seeking to rely upon consent for employee participation in a study where the employee has no real option of saying no could be considered to be compulsion. The WP29 needs to be thoughtful about not discouraging the legitimate use of consent by presenting it as impossible to lawfully obtain in too broad a set of circumstances.

SPECIFIC

The requirements listed on establishing the standard for specific consent highlight the challenge to effectively collect consent in a manner with which users can and will engage. We must avoid the presentation of dense information that a user must agree to before proceeding to the service, which they are seeking. However, the guidelines seem to present this as the preferred option.

Regarding point (ii), on the requirement for a separate opt-in for each purpose, we would like to emphasize that this is not required by the GDPR, especially if the purposes are related. Article 6 allows for consent to processing for "one or more specific purposes" - indicating that consent can be obtained for multiple specific purposes. For example, as per the above, 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. We note the position of the WP29 in relation to unrelated purposes, however for related purposes it would likely to be impractical for a user. We are also concerned by the use of "opt-in" in this language as the GDPR does not require an opt-in for consent and, in fact, the phrase "opt-in" is not used anywhere in the GDPR.

MINIMUM CONTENT REQUIREMENTS FOR CONSENT TO BE 'INFORMED'

Whilst we generally agree with the proposed list of information required for obtaining a valid consent, we would, like to point out that it would not always be practical for a controller to present all of this information on the user's screen as part of an affirmation of consent. This is especially true in cases where the screen is very small or there is not a visual user interface, i.e. voice controlled products. So while we welcome the WP29's acknowledgement of the benefit of a layered approach, we also believe that information such as the list of all organisations in the case of joint controllers is not appropriate for the consent notice.

HOW TO PROVIDE INFORMATION

We welcome the clarification that valid and informed consent can exist, even when not all the elements of Article 13 and/or 14 of the GDPR are mentioned in the process of obtaining consent. We understand that it means that the key requirement is that such information should be easily accessible to the user.

UNAMBIGUOUS INDICATION OF WISHES

The draft guidelines' view that "merely proceeding" cannot be regarded as an active indication of a user choice is perhaps unintentionally negative. Once a user is presented with sufficient information to make an informed choice, proceeding to use a service by means of a "next" or "continue" button or something similar may be entirely acceptable as meeting the requirements of consent. 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. It would be unfortunate if a seamless user experience were to be entirely sacrificed by placing what may be seen as obstacles in the way of users. This may be very similar to users' reaction to cookie gates previously.

CONSENT THROUGH ELECTRONIC MEANS

We welcome that the guidelines provide some liberty for controllers to develop a consent flow that suits their organizations and that is appropriate to the service. We equally welcome that the guidelines acknowledge the concern of click fatigue.

DEMONSTRATE CONSENT

It is important to recognise that the suggestion as a best practice that consent should be refreshed at appropriate intervals will very likely substantially increase consent fatigue. Asking a user to confirm something they have already confirmed, in addition to consenting to new or updated uses, will confuse the user and cause them not to engage. This requirement should be met by ensuring an easy means to withdraw consent.

EXPLICIT CONSENT

The draft guidelines describe a standard for explicit consent that is not supported by the text of the GDPR and that will likely be impractical at best or even unworkable. For example, requiring 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 can accept by clicking a button or turning on a setting. This would be in line with the ICO guidelines[1].

OFFERED DIRECTLY TO A CHILD

We consider the draft guidelines interpretation of Article 8 to be particularly restrictive and not supported by the actual text of the GDPR. It will be clear on its face whether a service is directed to children.

We are also not clear why an age of 18 is suggested when the GDPR has set the age for a minor at a maximum of 16 with an ability to lower. It should not be the case that sites should now seek to expressly exclude all users below 18 in order to minimise risk in this area. A more risk-based approach should be supported that takes account of the actual interest of the site to minors.

Furthermore, since consent can only be obtained from the child herself when he or she is above the age of consent, the WP29 seems to suggest that individuals above the age of consent must be provided with child-centred information. This should be reconsidered, as especially in the case of almost grown up teenagers, this could be highly counterproductive.

AGE

We welcome the relatively pragmatic approach the guidelines take regarding the verification of consent. It is our strong view that age verification should not lead to additional or excessive data processing. Establishing a real-world identity can be very challenging in practice and would imply processing a significant amount of data. Companies should be able to trust the honesty of their users, even when they indicate they are above the age of consent. Any interpretation to the contrary could trigger unnecessary data collection for millions of users, which would be contrary to Article 11 of the GDPR.

Regarding the method of verification, while credit card information are often used to collect such consent for services where it is anyway provided, other mechanisms should be available for service providers. Verification via email or via the parent's password (when the parent has an existing account with the service provider) are also robust mechanisms for both low and high-risk situations.

Last but not least, we support the call on the Member States to search for a harmonized solution on the age of consent. DIGITALEUROPE believes that the age for consent should be harmonised at 13 years old Well established research has demonstrated that it supports the public policy goal of digital inclusion[2]. A Harmonising the age of consent across the EU at 13 is also necessary, as imposing disproportionate measures create artificial barriers for children to participate online will prompt some to look for new ways to break the rule.

[1] Available at https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

[2] See Livingstone S, Helpster E. (2007) Gradations in digital inclusion: children, young people and the digital divide, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.455.5111&rep=rep1&type=pdf and London School of Economics (2017) Against raising the age limit for parental consent, available at http://blogs.lse.ac.uk/parenting4digitalfuture/2017/11/29/against-raising-the-age-limit-for-parental-consent/

CONSENT OBTAINED UNDER DIRECTIVE 95/46/EC

We welcome the assurance of the opinion that consent obtained under Directive 95/46/EC should remain valid. GDPR compliance comes with great expenses for businesses already. Checking all lawfully given consent under current privacy legislation would be a huge administrative burden for businesses. However if there are consent renewal policies in place based on the GDPR, this should be sufficient. All consent given under the former legislation will then be automatically checked.

--

For more information please contact:
Iva Tasheva, DIGITALEUROPE's Policy Manager
+32 2 609 53 12 or iva.tasheva@digitaleurope.org

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE's members include in total 25,000 ICT Companies in Europe represented by 60 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, Bose, Brother, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20