Brussels, 23 January 2018

EACB's views on the Article 29 Working Party draft Guidelines on Transparency and Consent under Regulation 2016/679

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

Introduction

The European Association of Co-operative Banks (EACB) welcomes the opportunity to provide the Article 29 Working Party (WP29) with its comments on the draft Guidelines on Transparency and Consent under the General Data Protection Regulation (GDPR).

Comments on the Guidelines on Transparency

Layered privacy statements/notices – paragraph 30, page 17

With regard to information 'fatigue' on the part of data subjects and as a general comment, the EACB fully supports the WP29 concept of a multi-layered notice format for data subject notices to ensure readability. We believe that the WP29 should encourage this concept given the prevalence of digital media. We do see benefits in adopting a multi-layered format where the initial notice contains the minimum information required by the EU legal framework and further information is available through links to the whole set of necessary information. In particular, EACB members support the idea of layered privacy statements and the possibility to use links instead of displaying a single notice on the screen.

This being said, we believe that the need to summarise the *'consequences of the processing in question'* should not restrict more customer-friendly design practices and result in the first layer being too detailed and long.

'Concise, transparent, intelligible and easily accessible' – paragraphs 8-9, pages 7 and 8

EACB members welcome the concept of 'the average member's level of understanding', which allows information to be targeted to the 'average member' without being too extensive or too simplified. However, contrary to the draft guidelines, we believe that compliance with the GDPR's transparency principle does not include a requirement for controllers to demonstrate their compliance by testing the intelligibility and the effectiveness of the information through user panels.

For the same reason, EACB members believe that the recommended best practice of providing detailed descriptions of the consequences of data processing, including those having *'the highest impact on the fundamental rights and freedoms of data subjects'*, goes considerably beyond the letter of the GDPR. In addition to increasing burden for the controller, we believe such practice could in effect worsen readability for the 'average member'.

Information to be provided to the data subject – Articles 13 & 14 – paragraph 19, page 12

As a general comment, EACB members believe that there is a contradiction between the obligation to provide concise and clear information (Art. 12 of the GDPR) and the amount of information to be provided to the data subject under Articles 13 and 14. Some new information obligations in the GDPR (compared to Directive 95/46/EC) are complex to disclose (for instance, 'the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period' might be difficult to explain). Moreover, it is often impossible to predict the actual contents of new services to be developed in the future. In addition, commercial organisations often cannot know their research purposes in advance. Moreover, the development of new services might also fall into category of business secrets, which are not disclosed until the release

of the new service. The Guidelines should clarify the distinction between essential information and possible further information contained in Art. 13(1) and (2) as well as Art. 14(1) and (2).

'Appropriate measures' – paragraph 22, page 13

At paragraph 22 it is stated that changes of the privacy notice must be communicated to the data subjects by hard-copy letter or e-mail. Whereas the intention of magnifying the visibility of the changes is laudable, we believe that notifications via letter or e-mail are not *always* required by the GDPR. The GDPR does not prescribe a specific form to communicate changes in the privacy policy, and we believe that insofar as other methods – e.g. a pop-up on the homepage or an updated leaflet in a bank's customer area – are effective, they should be considered sufficient.

Time for provision of information – paragraphs 24-25, pages 14-15

Another example where the draft Guidelines go beyond what is required by the GDPR regards the lack of flexibility on the timeframes within which the required information must be provided to the data subject. The GDPR gives a margin of flexibility in this regard, whereas the draft Guidelines tend to limit such timeframe by asking the data controller to justify *'why the information was provided at the time it was'* (the general one-month time limit to provide information may be curtailed).

Time of notification of changes to Article 13 and 14 information – paragraph 28, page 16

The draft Guidelines once again go beyond the GDPR's requirements. There is no obligation in the GDPR to remind the data subject at appropriate intervals about the information already given. The data controller is only required to keep the information available.

Other types of appropriate measures – paragraph 33 letter d, page 19

We suggest adding the word 'or' in the following sentence: '*oral explanations, **or** written explanations provided in hard or soft copy format*'.

Information on profiling and automated decision-making – paragraph 34, page 19

As we have already noted in our comments on the WP29's Guidelines on automated individual decision-making and profiling, we believe 'profiling' should not automatically be conflated with 'automated decision making'. While the latter can be based on the former, profiling does not always result in automated decision-making. We believe the GDPR does not include an obligation to provide information about the logic involved in profiling operations when these are not linked to *'legal effects concerning [the data subject] or similarly significantly affects him or her'*.

Other issues – risks, rules and safeguards – paragraph 35, page 19

As stated in the guidelines, publishing a DPIA, even partially, is not a legal requirement under the GDPR but is left to the controller's judgment. We strongly support this position. We believe that any recommendations or publishing requirements should be avoided. The publication of DPIAs, even partially, might be a source of risk for the data controller, e.g. in that they might include business secrets.

Information related to further processing – paragraph 40, page 21

Once again the draft Guidelines go too far compared with the GDPR requirements. The letter of the GDPR does not require data controllers to provide information on the compatibility analysis for further processing under a legal basis other than consent or national/EU law.

Exercise of data subjects' rights – paragraph 48, pages 23-24

EACB members are concerned about the draft Guidelines listing as 'poor practice example' the presence of a statement on a company's website inviting data subjects to contact the company's customer service to access their personal data. Such practice is not only perfectly legitimate but might also provide the most appropriate form of access in many circumstances. The GDPR does not contain an obligation for controllers to provide data subjects with forms for exercising their rights. As stated in the draft Guidelines, a data controller may wish to provide different modalities for the exercise of rights which are reflective of the different way in which data subjects interact with that data controller.

Exceptions to the obligation to provide information – paragraph 49, page 24

The best practice recommendation from the WP29 requires the data controller to again provide all the information (13.1/13.2 of the GDPR) when collecting additional data even if the data subject had already been informed of all the mandatory information, for instance six months ago.

This recommendation clearly goes beyond the requirement of the GDPR. In addition, we believe such requirement creates unnecessary duplication; transparency and control for the data subject can be better achieved by allowing the data subject to voluntarily seek the information already communicated.

Impossibility of providing the source of the data – paragraph 53, page 26

EACB members believe that it should be clarified that it is sufficient to mention the different sources in general. For the purpose of the general information obligation under Art. 14 of the GDPR, it is not necessary to name the specific data sources for the specific data subject.

Legitimate interest and information requirement – page 31

EACB members once again find that the information requirement indicated by the WP29 goes beyond the GDPR. Similar to DPIAs, a requirement to *'also provide the data subject with the information from the balancing test'* might be a source of risk for the data controller, e.g. in that the balancing test might include business secrets.

'Recipients' of the personal data and transfer of personal data to third countries – pages 32 and 33

Last but not least, EACB members believe that the draft Guidelines set too strict conditions for identifying 'recipients' and for listing all third countries to which the data will be transferred. We believe that the WP29's default position both for the 'recipients' (requiring information about *'the actual (named) recipients'*) and the details of the transfer to third countries (mentioning *'all third countries to which the data will be transferred'*) go beyond the GDPR requirements. For instance, the GDPR does not include an explicit requirement to name the specific recipients and to give reasons in case only categories of recipients are provided. The same applies for listing all third countries; the GDPR does not require to list all third countries in connection with information listed under Article 13 and Article 14. It should also be noted that the named subcontractors and

their locations may also be trade secrets of the controller. We also believe that an average member of the intended audience does not need to have this information at all. For this reason, we kindly ask to delete/change the wording.

Comments on the Guidelines on Consent

As a general comment, we wish to note that banks make little use of consent as a legal basis for their processing of customer data, which is rather based on the execution of a contract or pre-contractual measure; a legal obligation; and/or the legitimate interest of the controller. Nevertheless, in our view some aspects described in the draft Guidelines should be considered cautiously as they could be very restrictive of co-operative banks' practices.

Too strict consequences for controllers to refuse or withdraw consent

The draft Guidelines often state that it should be possible to refuse or withdraw consent without remarkable negative effects to the data subject, see examples in the table below:

- Page 8 '*consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of … significant negative consequences (e.g. substantial extra costs) if he/she does not consent';*
- Page 11 *'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'*;
- Page 12 *'[T]he data subject should be able to withdraw his/her consent without detriment. This means, inter alia, that a controller must make withdrawal of consent possible free of charge or without lowering service levels*';
- Page 9 *'The GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract. The two lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged and blurred'*.

This kind of interpretation is detrimental to the development of new data-related services or even the effective continuation of current services (for instance services financed with advertising fees). In a 'data-driven economy', data has become a 'means of payment', which can be used in buying different services for free or at lower price, where the service provider gets consent for the use of data in return.

A data subject always has control as to whether or not he or she wants to use such services, but it is up to the controller to decide what kind of service is provided. In some cases it is not even possible to provide a service at all without consenting (e.g. financial management tools based on own transaction data). EACB members believe that there should be a right balance between the interests of the data subject and those of the controller.

Imbalance of power – section 3.1.1., page 8

With regard to the imbalance of power in the employment context, EACB members believe that the draft Guidelines go too far where they state that in the employment context it is unlikely that a data subject gives his/her consent freely. Indeed, as also pointed out in the following paragraph of the draft Guidelines and in the example 5, there maybe situation when it is possible and not unlikely that employees consent to data processing freely.

Conditionality – section 3.1.2., pages 9-10

Data processing for marketing purposes, p. 10

We would like to highlight that a controller might seek to process personal data for marketing purposes under the legitimate interest legal basis in Article 6(1)(f). Indeed, Recital 47 of the GDPR states that 'The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest'.

However, the draft Guidelines – notably paragraph 3.1.2. illustrated by example 6 – seem to imply that if processing for marketing purpose cannot be carried out under the lawful basis Article 6(1)b (contract), only consent (6(1)) should apply.

We believe this ambiguity, which runs against the letter and the intent of the legislator in the GDPR, should be rectified to make it explicit that the processing of personal data for marketing purposes is possible under the lawful basis of Article 6(1)(f), as stated in Recital 47. By the same token, we believe example 6 should be removed.

With regard to Art. 7(4) of the GDPR, the draft Guidelines state that consent to data processing must not be counter-performance of a contract; further on page 10, the draft Guidelines state that the offering of alternative service-models with and without consent to data processing requires that both services must be genuinely equivalent, including no further cost. However, the GDPR does not provide a basis for such strict requirements. Art.7 (4) of the GDPR can and should be interpreted in such way to allow alternative service-models with more differences in their conditions.

Granularity – section 3.1.3., page 11

EACB members invite caution about the draft Guidelines' statement that the GDPR requires multiple consents for multiple processing purposes. Although this might be true in some circumstances, an excessive level of granularity might restrict a processor's possibility to define the actual content of the service it provides. Processors should be able to define the service provided, which might involve a bundle of processing operations and therefore require consent to all related purposes.

Detriment – section 3.1.4., page 11

According to the statement in this section, it would appear that any minor detriment in case of withdrawal of consent would render consent void. EACB members believe that this is too restrictive and should be changed/clarified.

Various business models depend on the provision of goods or services for free, provided that the customer/user consents to the processing of his/her personal data for marketing purposes. Instead, the 'detriment' for the data subject resulting from a withdrawal of his/her consent must be significant to render the consent void (see e.g. *Feiler/Forgó*, EU-DSGVO p. 109). Accordingly, the word '*any*' should be replaced by '*significant*'.

How to provide information – section 3.3.2., page 15

EACB members believe that the request to test the information given for the collection of consent with a panel of users, to prove that consent is given in an 'informed' way, goes beyond the requirements of the GDPR.

Obtaining explicit consent – section 4, page 19

EACB members find that checkboxes provide an efficient means for both parties (data controller and data subject) to signal and register explicit consent. We therefore urge the WP29 to include checkboxes in the sample list given in the fourth paragraph of section 4 of the draft Guidelines.

EACB members believe that the example of two-stage verification as a way to make sure that explicit consent is valid is too burdensome in practice both for a data controller and for a data subject and does not support the development of modern sophisticated services.

Demonstrate consent – section 5.1., page 20

EACB members welcome the WP29's recognition that the GDPR does not specify the time limit for how long consent will last. As well-stated, how long consent lasts will depend on the context, the scope of the original consent and the expectations of the data subject.

The WP29's recommendation to refresh the consent at appropriate intervals as a best practice should be interpreted as a possibility/option for the data controller and not as an obligation. Indeed, data controllers should have flexibility to determine when consent needs to be refreshed depending on the circumstances. Unnecessary renewals might lead to bad customer experience and increase the risk of consent fatigue.

Interaction between consent and other lawful grounds in Article 6 GDPR – section 6, page 22

We believe that the GDPR does not provide that data processing cannot be based on more than one legal grounds. Even though the purposes of data processing should not be changed later on, there is no compelling argument why data processing should not be based on several legal grounds, including the explicit consent of the data subject.

Age – sections 7.1.3. and 7.1.4., pages 25-26

On page 26 last paragraph it is stated that the consent given or authorised by the holder of parental responsibility expires once the data subject reaches the age of digital consent and, from that day forward, the controller must obtain valid consent from the data subject him/herself. Considering that the age of digital consent is set at 14 years in some Member States, one would face the paradox of consent given or authorised by the parents of the minor becoming void while the minor still requires parental approval for many contracts. There is no basis for such a view in Art. 8 of the GDPR. According to civil law in some Member States, the consent of the holder of parental responsibility remains effective when the minor reaches full legal capacity. We believe that the paragraph should be modified so that the consent given or authorised by the holder of parental responsibility remains valid after the data subject reaches the age of digital consent, and that therefore the consent must not be repeated by the data subject at this point. This is also not detrimental for the data subject, as he/she is still free to withdraw his or her consent at any time.

Moreover, the Guidelines go beyond the Regulation when they state that in high-risk cases the controller should make checks to verify the user's age:

- *'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'.*
- *'In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor'.*
- *'Conversely, in high-risk cases, it may be appropriate to ask for more proof'.*

- *'For example, a parent or guardian could be asked to make a payment of €0,01 to the controller via a bank transaction, including a brief confirmation in the description line of the transaction that the bank account holder is a holder of parental responsibility over the uses'.*

Consent obtained under Directive 95/46/EC – section 8, page 30

The spirit of Recital 171 of the GDPR points towards a need to preserve consent obtained prior to the application of the GDPR so long as the spirit of the GDPR is protected. We believe that this should result in simplified procedures that aim to effectively inform data subjects rather than in a duplication of requests for consent. In this context, for instance, rather than having to seek new consent from scratch, we believe controllers should be able to demonstrate the data subject's consent by sending its existing clients new information about processing according to Articles 13 and 14 of the GDPR.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department Retail Banking, Payments, Financial Markets (marieke.vanberkel@eacb.coop)
- Ms Chiara Dell'Oro, Adviser, Consumer and Retail Banking (chiara.delloro@eacb.coop)

We hereby consent to the publication of personal data contained in the document.