Brussels, 23 January 2018

AMICE contribution to the Article 29 Working Party's draft Guidelines on Transparency and Consent under Regulation 2016/679

About AMICE (Association of Mutual and Cooperative Insurers in Europe)

AMICE is the voice of the mutual and cooperative insurance sector in Europe. The Brussels-based association advocates for appropriate and fair treatment of all mutual and cooperatives insurers in a European Single Market. It also encourages the creation and development of innovative solutions for the benefit of European citizens and society.

Mutual and cooperative insurance follows the principles of solidarity and sustainability and is characterised by customer-membership and a democratic governance. The mutual business model, with its focus on using surpluses for the benefit of its members, is the natural way to provide insurance.

Mutual and cooperative insurers have a market share of more than 30% of the European insurance sector, with more than €420 billion in premiums written and over 410 million policyholders across Europe.

Introduction

AMICE welcomes the opportunity to provide feedback on the Article 29 Working Party's draft Guidelines on Transparency and Consent under the General Data Protection Regulation (GDPR).

Comments on the Guidelines on Transparency under Regulation 2016/679

"Concise, transparent, intelligible and easily accessible" (paragraphs 8-9)

AMICE 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.

- *"The requirement that information is "intelligible" means that it should be understood by an average member of the intended audience. This means that the controller needs to first identify the intended audience and ascertain the average member's level of understanding." (point 8)*

However, the recommended best practice of providing a detailed description of the consequences of data processing, including those having "the highest impact on the fundemental rights and freedoms of data subjects" goes beyond the level 1 text of the GDPR. The determination and description of "the highest impact" would be in practice a quite demanding task for a data controller. Moreover, "the highest impact" might also be a subjective concept.

- *"Such a description of the consequences of the processing should not simply rely on innocuous and predictable "best case" examples of data processing, but should provide an overview of the types of processing that could have **the highest impact** on the fundamental rights and freedoms of data subjects in relation to protection of their personal data." (point 9)*

Information to be provided to the data subject – Articles 13 and 14 (paragraphs 11 and 19)

AMICE believes that there is a contradiction between the obligation to provide concise and clear information (Article 12 of the GDPR) and the amount of information to be provided to the data subject under Articles 13 and 14 of the GDPR. In particular, it is often impossible to predict the actual contents of new services to be developed in the future. In addition, commercial organisations do not often know their research purposes in advance. One cannot avoid "information fatigue", if organisations are obliged to provide these details. The development of new services might also fall into the category of business secrets, which are not disclosed until the release of a new service. Therefore, the guidelines should clarify the distinction between essential information and possible further information contained in sub-articles 1 and 2 of Articles 13 and 14 of the GDPR.

Layered privacy statements / notices (paragraph 30)

AMICE supports the idea of layered privacy statements (point 30) and the possibility to use links instead of displaying a single notice on the screen. Nevertheless, we believe that the requirement to summarise the consequences of the data processing should not restrict more customer-friendly design and result in the first layer being to detailed and long.

- *"With regard to the substantive information which may be included in the first layer of the privacy statement/ notice, WP29's position is that this should always contain information on the processing which has the most impact on the data subject and processing which could surprise the data subject. Therefore, the data subject should be able to understand from information contained in the first layer what the consequences of the processing in question will be for the data subject" (paragraph 30)*

Recipients of the personal data and transfers to third countries (pages 32 and 33)

AMICE members are concerned that the draft Guidelines set too strict conditions for identifying "recipients" (requiring information about "*the actual (named) recipients*") and for listing *all* third countries to which the data will be transferred. These requirements go beyond the level 1 text of the GDPR. The GDPR does not require to name specific recipients and to give reasons in case only certain categories of recipients are provided. Similarly, the GDPR does not contain an explicit requirement to list all third countries in connection with the information listed under Articles 13 and 14 of the GDPR. It should be noted that the named subcontractors and their locations may also be trade secrets of the controller. An average member of the intended audience does not need to have this information at all. Therefore, AMICE suggests the deletion of the following wordings.

- *"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" (page 32)*
- *"In accordance with the principle of fairness, the information should explicitly mention all third countries to which the data will be transferred" (page 33)*

Information that must be provided to a data subject and legitimate interest (page 31)

AMICE members are concerned that the requirement "to provide the data subject with the information from the balancing test" goes beyond the level 1 text of the GDPR. It should be emphasized that this should only be a voluntary action of the data controller.

- *"As a matter of best practice, the data controller should also provide the data subject with the information from the balancing test" (page 31)*

Comments on the Guidelines on consent under Regulation 2016/679

Strict consequences for data controllers to refuse or withdraw consent

The draft Guidelines foresee the possibility for data controllers to refuse or to withdraw the consent without any significant negative effects on the data subject (see examples below). This interpretation is detrimental to the development of new types of data-related services or even the effective continuation of current services (for instance, services financed with advertising fees). Nowadays, in a "data-driven economy" data has become a "means of payment" which can be used in buying different services for free or at a lower price, where the service provider gets consent for the use of data in return.

A data subject has always control as to whether or not he/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 consent. There should be a right balance between the interests of the data subject and those of the controller.

- *"consent can only be valid if the data subject is able to exercise a real choice, and there is… no significant negative consequences (e.g. substantial extra costs) if he/she does not consent" (page 8)*
- *"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 11)*
- *"Furthermore, the 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 21)*
- *"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." (page 9)*

Granularity of consent (page 11)

The requirement to seek separate consent for each purpose for processing instead of consenting to a bundle of processing purposes might restrict the processor's possibility to define the actual content of the service he/she provides. Processors should be able to define the service provided and seek sufficient consent for these bundled processing operations (for each of them). It is up to the data subject to accept or reject all of these processing purposes. In addition, separate consent for each processing purpose might lead to a "consent-overload".

- *"A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR." (page 11)*

Obtaining explicit consent (page 19)

AMICE believes that the two-stage verification of consent is too burdensome in practice both for the data controller and the data subject and does not support the development of modern sophisticated services even though it is one of the options for obtaining explicit consent.

- *"If the data subject agrees to the use of this data, the controller asks him or her for an email reply containing the statement 'I agree'. After the reply is sent, the data subject receives a verification*

link that must be clicked, or an SMS message with a verification code, to confirm agreement." (page 19)

Demonstrate consent (page 20)

The WP29's recommendation to refresh the consent at appropriate intervals as a best practice should be interpreted as an option for the data controller rather than an obligation. Data controllers should have the flexibility to decide when the consent needs to be refreshed depending on the circumstances. Unnecessary renewals of consent might lead to a bad customer experience if they happen too often.

- *"WP29 recommends as a best practice that consent should be refreshed at appropriate intervals. Providing all the information again helps to ensure the data subject remains well informed about how their data is being used and how to exercise their rights." (page 20)*

Age (pages 25-26)

AMICE considers that the draft Guidelines go beyond the level 1 text of the GDPR 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 user." (pages 25-26)*

Consent obtained under Directive 95/46/EC (page 30)

The draft Guidelines provide a very strict interpretation of consent obtained prior to the application of the GDPR. AMICE believes that controllers should be able to demonstrate the data subject's consent by sending customers new information about processing according to Articles 13 and 14 of the GDPR.

- *"For example, as the GDPR requires that a controller must be able to demonstrate that valid consent was obtained, all presumed consents of which no references are kept will automatically be below the consent standard of the GDPR and will need to be renewed." (page 30)*