AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Working Party 29 guidelines on Transparency under Regulation 2016/679

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2016, directly supports more than 4.5 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Contents

General remarks

US businesses, like many other companies throughout Europe, are today hard at work implementing the GDPR. One focus of this effort has involved updating and expanding privacy notices and other information in order to meet the GDPR's highly detailed transparency-related requirements.

Our members, also like companies across Europe, arrive at this challenge from a wide range of backgrounds, sizes and sectors. Accordingly, the information these companies provide and how they provide it will necessarily also differ: from small enterprise to large ones; across multiple industries as diverse as pharmaceutical development, chemical manufacturing, and online services; and across technologies and mediums. Therefore it is critical that the transparency standards set out in the GDPR are interpreted by the Working Party 29 guidelines in a technology-neutral way, and in a manner that provides controllers with the opportunity to exercise judgment when selecting what, when and how to communicate with data subjects. After all, controllers, more than anyone else, understand their own relationships with data subjects, and the circumstances in which they are operating.

The Article 29 Data Protection Working Party (hereafter 'WP 29') Guidelines on transparency under Regulation 2016/679 (hereafter 'draft guidance') does in fact make clear that controllers should exercise some discretion and judgment to provide notices appropriately, and we welcome such clarity. In addition, it would be welcome if the WP 29 could give some clarification on how the controller can fulfil the requirement to provide the identity of the controller. Especially in large group companies, the processing of data is often organised around global processes. To the extent there is clarity on what type of companies are controllers, efficient means to communicate with them, and adequate means for data subjects to exercise their rights under the GDPR, especially if the controller has measures in place such as Binding Corporate Rules, alternative ways than to list all the applicable legal entities should be preferred.

It is concerning that the draft guidance in some aspects are highly prescriptive and overstretch obligations under the GDPR which risks to results in an 'information fatigue:

- **More flexibility is needed** - Certain parts of the guidance are highly prescriptive, and do not leave sufficient latitude for discretion on the part of controllers to judge how best to present information to data subjects given their specific circumstances. As a consequence, they may not survive the test of time. For example, the draft guidance emphasises that layered notices in applications should be no more than 'two taps away'. This recommendation may date rapidly if

smartphone users move towards voice-based interfaces, or if the applications concerned are embedded in Internet of Things (IoT) devices instead of touch-screen devices.

- **The risk of information fatigue** - the draft guidance also at times reaches further than the requirements of the GDPR, which could undermine the careful balance struck by legislators and increase the 'information fatigue' that the WP 29 rightly acknowledges is a threat to transparency in data protection. This is particularly true in cases where the guidance appears to recommend privacy reminders or notifications that go far beyond what the GDPR requires. In particular, the draft guidance repeatedly cites the principle of 'fairness' as grounds for specifying types of information that should be provided to data subjects that exceed the explicit informational requirements of the GDPR (eg as set out in Articles 13 and 14). The principle of fairness may, in specific cases, and depending on the circumstance, require provision of additional information – but not in a rote way that applies *en masse* to every data controller and every relationship with data subjects. Had that been the drafters' intent, the drafters would have included those types of information in the GDPR.

Below we outline our comments on the draft guidance along these two main concerns.

Comments on the draft guidance

Elements of transparency under the GDPR

- On page 8 (para. 9), the WP 29 states that 'as a best practice, in particular for complex, technical or unexpected data processing, […] controllers should not only provide the prescribed information under Articles 13 or 14, but also separately spell out in unambiguous language what the most important consequences of the processing will be: in other words what kind of effect will the specific processing described in the privacy statement/notice have on a data subject'. To avoid introducing a new disclosure obligation on organisations not found in the GDPR, the guidance should qualify the scope of the recommended 'best practice' of spelling out potential risks and harms associated with processing by clarifying that controllers must exercise their judgement in how to provide effective and actionable transparency concerning the possible consequences of their processing, consistent with the GDPR.

- The draft guidance sets out recommendations that will age quickly. Perhaps the clearest example of this is in para. 10, which suggests that information should always be made available on app stores before apps are downloaded, and that information should also be made available within apps within 'two taps'. These broad prescriptions allow little room for alternatives – for example, 'welcome screens' in apps that can present necessary information before data collection commences, even where information is not provided on app store pages, or highly streamlined apps where information reaches users through a direct 'push notification' rather than in a menu two clicks beneath the main interface. This guidance will be a resource for controllers over many years, and the technologies of today will not necessarily be the most effective tomorrow. Consider connected cars, for example, which often include apps; here, requiring information to be buried under multiple taps, and/or on non-existent app store pages, may be a far inferior method of information delivery in comparison to voice messages or other creative solutions available in the coming years. The draft guidance should be revised to encourage controllers to think more

creatively along these lines, with the goal of always ensuring data subjects understand how data about them will be processed.

- The draft guidance also makes prescriptive recommendations that do not take context into account. For example, the statement that words like 'may' or 'might' 'should be avoided' in paragraph 12 is inflexible, and fails to account for scenarios where data processing is conditional (for example, an airline might say that data 'may' be shared with governments – but only where that sharing is mandated under applicable laws, which may not be true in every case). Likewise, the draft guidance takes the position that phrases like 'we may use your personal data to offer personalized services' are always unclear – without considering the other information provided to the data subject, or their expectations based on their other interactions with the controller. We encourage the draft guidance to be more nuanced to accommodate the diversity of scenarios and fact patterns regulated by the GDPR.

- On page 11 (para. 16), the WP 29 notes that under Article 12.1, 'information may be provided orally to a data subject on request, provided their identity information is proven by other (i.e., non-oral) means'. We recommend to clarify that proving a data subject's identity through 'other, i.e., non-oral means' precludes verbal assurances that 'I am so and so' but does not preclude confirming or proving identity through voice recognition. In addition this statement is confusing as it refers to the data subjects' rights of art. 15 and on.

Information provided to the data subject – Articles 13 & 14

- The draft guidance states that changes to existing privacy statements should be always communicated 'by way of an appropriate modality (e.g. email/hard copy letter etc.) specifically devoted to those changes' (see para. 22). Whereas we agree that major changes should indeed be communicated with a clear separate message, this is not appropriate for all minor changes as this would result in information overload for the data subjects.

- The draft guidance contemplates regular 'privacy reminders' that exceed what the GDPR requires. The recommendation for reminders to be sent 'at appropriate intervals' to data subjects even where the privacy statement does not change (see para. 28) should be moderated. Data subjects have relationships with hundreds of businesses in the course of a normal year; if they received an annual reminder from each, they would receive potentially one to several reminders every day. This would quickly undercut any value intended by such reminders. Therefore, the draft guidance should clarify that the question of whether and in what intervals 'reminder notices' should be sent to individuals even when there have been no material changes to the privacy statement/notice should be left to the judgment of the organisation. A decision on that point should be based on the organisation's assessment of whether such reminders would be useful and not burdensome and intrusive to the individual. Furthermore, where no changes to a privacy policy/notice have occurred, organisations should also be able to rely on the ability of individuals to find such policies/notices in an appropriately identified location online.

- The draft guidance advocates a layered privacy statement with the first layer always containing all consequences of the processing to the data subject. The suggested layered approach indeed is best practice and substantive adverse consequences should be communicated in the first layer statement. However, the draft guidance stipulates that 'the data subject should be able to

understand from the information contained in the first layer what the consequences of the processing in question will be' (para. 30). As many processing activities will not have any adverse consequences for the data subjects, it would again amount into an information fatigue for the data subject if all (even insubstantial) consequences would be embedded in the first layer. We therefore suggest limiting this obligation to processing activities with substantial adverse consequences for the data subjects.

Comments on Information related to further processing

The draft guidance supports identifying details of compatibility determinations (para. 40). The GDPR sets out rules enabling the processing of data for purposes beyond the original purpose for which data is collected where that processing is compatible (see Article 5(1)(b) and Article 6(4) in particular). And while it is clear that controllers should notify data subjects where further processing is carried out, it does not, in either Article 13, 14, or elsewhere, mandate that controllers notify data subjects of the actual analysis of compatibility. This requirement goes beyond the GDPR; publication of this technical information would only undercut the goals of clarity and simplicity (which are also crucial for transparency), and add little, if any, value for data subjects. There are many examples of central databases which are from the outset on intended to share their personal data for other, yet not specifically known purposes, such as an internal contact database, or basic employment related information. It would be information overload to inform all data subjects each time of such other (compatible) use, other than in the context of the information requirements of art. 14. We therefore recommend to delete the paragraph suggesting that organisations must provide their compatibility analyses to individuals to comply with the GDPR transparency requirements.

Exercise of data subjects rights

On pages 23-24 (para. 48), the WP 29 addresses the appropriate modalities for facilitating the exercise of individuals' rights under the GDPR. On page 24, it provides a 'Good Practice Example' and a 'Poor Practice Example.' These examples should be clarified in the draft guidance in terms of the conclusions that one is good and the other poor, as follows:

- The 'Good Practice Example' is only good if alternative modalities not requiring filling out a form are also provided.
- The 'Poor Practice Example' is only poor if the statement on the website does not contain the relevant contact information for the customer services department.

Exceptions to the obligation to provide information

- The WP 29 states in its 'Example' (para. 49) regarding Article 13 exceptions that an individual must be provided with new information under Art. 13 when there is a new purpose of processing (here the messaging service) and that, as a matter of best practice, all the information under the notice requirement should be provided again even if individuals received the information before. This directly contradicts Article 13.4, which provides that paragraphs 1, 2 and 3 of Article 13 shall not apply 'insofar as the data subject already has the information.' In order to align the draft guidance with Article 13.4, the statement/example should be removed. The draft guidance should clarify

that providing such old information should be left within the discretion of the controller if it finds that this would be useful and not undermine overall transparency.

- On page 28 (para. 57), the WP 29 states that where a data controller 'seeks to rely on the exception in Article 14.5(b) on the basis that provision of the information would provide a disproportionate effort, it should carry out a balancing exercise to assess the effort for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information.' However, the GDPR does not require this kind of risk assessment or balancing test in this context. The reference to a balancing exercise between the efforts involved in providing information against the impact of not providing the information should be removed.

Schedule – Information that must be provided under Articles 13 or 14

- The draft guidance advocates for identifying the details of balancing tests when data is processed based on legitimate interests (p.31). The GDPR sets out that where a legitimate interest under Article 6 is the basis of processing, this should be notified to data subjects (Article 13(1)(d) and Article 14(2)(b)). However, the draft guidance again goes further and states that it would be best practice for controllers to make available information on the 'balancing test' required in order to determine whether legitimate interests can justify processing. Again, this would contribute to information overload, undermining goals of clarity, brevity, and transparency in notices.

- The draft guidance argues identifying all recipients of personal data should be general practice (p.32). The GDPR is clear that controllers should notify 'recipients (or categories of recipients) of personal data' to data subjects (Article 13(1)(e) and Article 14(1)(e)). However, the draft guidance interprets this such that the 'default position' should be that controllers should regularly identify each specific recipient. In cases where controllers have relationships with a wide array of counterparties – and particularly in cases where those counterparties change frequently – this could, if it becomes a general practice, easily result in overload to data subjects, without adding significantly to their understanding of how their data will be used and shared. We therefore recommend to amend this interpretation to reflect two co-equal options of disclosing 'recipients' or 'categories of recipients' and remove the new requirement of proving fairness and the definitions of what 'categories' means.

- The draft guidance argues that all countries to which personal data will be transferred must be listed (p. 33). This goes beyond the requirement of the GDPR, which requires the controller only to notify 'the fact that the controller intends to transfer personal data to a third country' to data subjects (Article 13(1)(f) and Article 14(1)(f)). This is particularly onerous as the list of countries to which personal data may be transferred may change over time – for instance, because an organisation appoints new data processors, or because the list of affiliates of such organisation changes. Again, this will likely result in information overload for the data subjects. We therefore recommend to delete the statement that controllers must explicitly mention all third countries to which data will be transferred.

- On page 35, in the box on 'source from which the personal data originate', the WP also adds additional requirements not found in the GDPR. Thus, while Article 14.2(f) only requires provision of information on 'from which source the personal data originate, and if applicable, whether it

came from publicly accessible sources,' the WP 29 adds that the information should also include information on 'the nature of the sources' such as 'types of organisations/industry sector' and 'where the information was held (EU or non-EU)'. We recommend to delete the additional requirements for source disclosures that are not found in Article 14.2(f).