Legal **Geek** Sp. z o.o.
ul. Obrońców Westerplatte 2-4/1
81-706 Sopot
NIP: PL 5862305970

Feedback on Guidelines 4/2019 on Article 25

Data Protection by Design and by Default

Sopot (Poland), 16. 01. 2020

The Guidelines will be referred to as „**Document**".

<u>Section 2</u>

We suggest adding a full text of Art. 25 of the GDPR so that the Document is more comprehensive. It would also make it easier for readers to refer to the article in question within the Document – without the need to reach for the GDPR.

<u>Section 2.1.1 → 7</u>

„The controller shall ***(1) implement appropriate technical and organisational measures*** *which are designed to implement the data protection principles* ***and (2) integrate the necessary safeguards*** *into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.* ***Both appropriate measures and necessary safeguards*** *are meant to serve the same purpose of protecting the rights of data subjects and ensuring that the protection of their personal data is built into the processing".*

It is often mentioned within the Document that the controller shall implement appropriate technical and organisational measures **as well as** integrate the necessary safeguards. Such clear division into these two categories is especially visible in Section 2.1.1, where the implementation of the measures is mentioned as the first obligation, and integration of the safeguards as the second one. It is also clearly stated in (10): *„safeguards act as a* ***second tier*** [author's note: as opposed to the term „measures" discussed in (8) and (9), which is being treated as the first tier] *to secure data subjects' rights and freedoms (...)*".

Meanwhile, according to Art. 25 (1) of the GDPR:

1. *(...) the controller shall, (...) implement appropriate technical and organisational measures, (...)* ***which are designed <u>to</u>*** *implement data-protection principles, (...)* ***and <u>to</u> integrate the necessary safeguards*** *into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*

Therefore, appropriate technical and organisational measures need to be designed in such a way that they:

1. implement data-protection principles in an effective manner;
2. integrate the necessary safeguards.

Separating the integration of the necessary safeguards as an activity that is different than implementing appropriate technical and organisational measures, which seems to be the case in the Document, does not correspond to the actual wording of the abovementioned provision. In fact, there is one main obligation regarding the measures, and safeguards are only a part of these measures. Referring to this obligation using the designation „measures and safeguards" may be misleading. It also suggests that they are in fact two very different things.

It may further lead to confusion as to which of the means undertaken by the controller shall be classified as measures, and which as safeguards. It seems to be the case in (11), where pseudonymization is mentioned as an example of both technical measures **and** safeguards.

<u>Section 2.1.3 → 22</u>

*„****Existing standards*** *and certifications may play a role in indicating the current „state of the art" within a field.* ***Where such standards exist, controllers should take these into account in the design and implementation of data protection measures***".

The word „standard" can be understood as a common practice. Therefore it is worth to indicate that the Document refers to practices verified by trusted entities such as relevant public authorities or courts. Also, it is worth mentioning that it usually takes some time for a new, better solution to become a standard. Therefore, existing standards should be taken into account, but they should also be verified by the controller before implementing them into a solution – it might be good to point it out in the Document, as the current wording of this paragraph suggests that such standards are not meant to be questioned.

Section 2.2 → 53

„Article 25(2) further states that personal data shall not be made accessible, without the individual's intervention, to an indefinite number of natural persons. ***The controller must by default limit accessibility and consult with the data subject before publishing or otherwise making available personal data about the data subject to an indefinite number of natural persons****"*.

The sentence in bold should apply in case of actions that are not the result of individual's intervention. The current wording of the sentence might suggest that despite the quoted article 25(2), the controller must consult data subjects before publishing their data even when the action has been initiated by the data subject himself.

If that remark is not accepted, we suggest adding an example of an action undertaken by the data subject using a solution provided by the controller. In case of opinions on products in online shops or comments on blog posts, it is sufficient for the controller to use proper wording on the buttons which are used to publish the comment. For example, instead of using the word „send" on the button, the controller should use a word „publish" – so that it is clear for the user that his data connected with the comment (such as a nickname and the comment's content) will be visible on the website, and not for example sent to the blog or shop owner.

Section 3 → 61 → Example

- *„The controller therefore provides information in a* ***multi-layered manner*** *(...)."*
- *„(...)* ***Links to other pages*** *are provided to further explain the concepts in the policy"*.

A common understanding of such statements may encourage controllers to create multiple subpages that users have to go through in order to get to the desired information. We suggest removing the word „multi" and underlining that also within the privacy policy itself (and not only within the webpage, as mentioned further in the Document), the user should be only one click away from the desired information. Other approaches may lead to hiding certain information from the user in the hope that such a long procedure of clicks discourages him from looking into it. Further information on the problem can be found in the deliberation of the French CNIL's restricted committee of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, where the committee has found that it should not be acceptable to disseminate important information across several documents that are referred to by links or buttons.

- *„The controller also makes sure that the information is provided in a **multi-channel** manner, providing **video clips** to explain the most important points of the information".*

This measure (and especially the example of a video clip) seems to be excessive and unrealistic. As long as a privacy policy is prepared according to the principles mentioned in the Document (above the example), in most typical cases it should be enough – unless some more intricate processing operations take place. It is also important to notice that mobile users may be charged with additional transfer costs for downloading the data necessary to display the video. Perhaps a better example of a multi-channel manner would be a graphic form of information which is easier to download.

- *„(...) generally a privacy policy on the website alone is not sufficient for the controller to meet the requirements of transparency. The controller therefore designs an information flow, presenting the data subject with relevant information within the appropriate context using e.g. **informational snippets or pop-ups**".*

Using informational snippets or pop-ups each time when data processing takes place may cause information fatigue and may result in overwhelming actual functions of the website or a solution with information on data processing.

It is worth mentioning that (32) of the GDPR states in relation to consent:

„If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise ***and not unnecessarily disruptive to the use of the service for which it is provided****”.*

The Controller has to fulfil strict requirements while obtaining consents and yet it is explicitly stated that the whole process should not be unnecessarily disruptive to the **use** of services. Accordingly, it can be assumed that this requirement shall pertain also to other aspects of communication with the user.

Pop-ups or excessively long information (in relation to the actual function) can significantly worsen the usage of the website, and especially so while using mobile devices. Given that nowadays most users use mobile devices to browse the Internet, it is important to take user experience into account.

What is more, informational snippets or pop-ups by definition are condensed and do not contain full information on the topic. At the same time, they might discourage the user from looking into the full version. Hence, the user will actually be less informed than in the case of sending him directly to the concise, clear and understandable privacy policy. Also, given the popularity of privacy policies as main external documentation on data processing, the user might get confused as to which information on data processing are relevant for him – informational snippets here and there coexisting with a privacy policy can cause informational chaos.

Therefore, we suggest changing the example into a simple reference to privacy policy (with a link to it) in crucial places such as below a contact form on the website, or below the checkbox to sign up for a newsletter.

Section 3 → 63

- *„Consent withdrawal – the processing shall facilitate withdrawal of consent. Withdrawal shall be as easy as giving consent. If not, any given consent is not valid”.*
- *„Balancing of interests –* ***where legitimate interest is the legal basis****, the controller must (...)”*

It should be indicated in the first sentence, that it applies where the consent is the legal basis – as it has been made in relation to the legitimate interest in the second sentence.

It is important, as controllers overuse requests for consent when the processing should take place on a different legal basis. For example, at the end of the path to purchase in online shops they often insert a checkbox, which states that the buyer agrees on using his data for the purpose of the realisation of the order. In such a case, the checkbox is excessive, because another legal basis for processing is appropriate (art. 6(b) of the GDPR). When compared with the sentence about balancing the interests, it seems as if obtaining consent at some point is always necessary, since its withdrawal is being mentioned without any restriction.

Section 3 → 71 → Example

*„The subject's date of birth and **phone number** are not necessary for the purchase of the product. This means that these cannot be required fields in the web form to order the product."*

Some of the courier companies require a phone number of a recipient in order to arrange the exact time of the delivery. Whenever the customer chooses such a company in the delivery method option in the online shop (or when such option is the only one available), requiring a phone number is justified – therefore the Document is too categorical in this regard.

Section 3

Every principle mentioned in Art. 5 (1) of the GDPR is further discussed in the Document. However, a provision of Art. 5 (2) can also be treated as a separate principle – especially given the title of the Art. 5 as a whole („**principles** relating to the processing of personal data") and the fact, that each principle mentioned in subs. 1 has a name attributed to it between quotation marks, which is the case for accountability as well. The placement of this provision at the beginning of the GDPR along with other principles suggests that it is equally crucial to have accountability in mind in the design and implementation process.

Therefore, although it is mentioned in the Document that controller should be able to demonstrate compliance with all of the other principles, it is worth to accentuate it more at the end to underline the importance of accountability – by adding another section similar to ones that pertain to other principles.

As for a practical example demonstrating implementation of accountability, we can suggest an administrator's panel for a website in which (among other functions) users can agree to receive marketing information on their e-mail address. In such case, administrator's panel should be designed in such a way that it allows the controller to obtain information on when the consent has been collected, what is it that the user consents to and on which e-mail address the user wishes to receive marketing information.