Spolek pro ochranu osobních údajů

**Comments on the EDPB's draft "Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them"**

We welcome the opportunity to present our comments to the recently published EDPB draft Guidelines 03/2022 on Dark patterns (Guidelines).

## General comments

We greatly appreciate the EDPB for preparing this comprehensive opinion. It is really very complex and addresses a number of issues. At the same time, it is focused to the very current topic of abusing the position of social networks towards their users by using dark patterns. We therefore consider this opinion to be very beneficial.

Nevertheless, we need to point out a few general issues. In particular, it seems to us that the Guidelines focuses mainly **on the largest social networks (platforms)**, on which it places - quite rightly - relatively strict requirements, partly because they carry out extensive processing of their users' personal data. However, it should be noted that **there are a number of smaller European social networks operating in the EU** which are far from posing such a risk to their users. In our opinion, it would not be appropriate to impose requirements on these smaller social networks providers comparable to giants with billions of euros in budgets. At the same time, some specific requirements set out in the Guidelines - according to the practical experience of our members, who work for smaller social networks - are relatively difficult to implement (both in terms of time and financial requirements).

In addition, in some examples, the Guidelines categorically identify as dark patterns such situations, which are common in practice (see, for example, Example 5 in point 42). It should be emphasized that these cases shall be identified as dark patterns only if there are special circumstances justifying such an assessment.

## Specific comments

In Paragraph 13 EDPB states: *"If refusing consent leads to a denial of the service, it cannot be considered as freely given, granularly and specific, as the GDPR requires. Consent that is "bundled" with the acceptance of the terms and conditions of a social media provider does not qualify as "freely given"."*

We believe that this issue cannot be assessed in such a categorical way. Especially for smaller services that are offered free of charge, a situation may arise where for the proper functioning of the service it will be necessary to obtain consent to the processing of personal data (e.g. for processing special categories of data) and without this consent the service provider will not be interested in such a user to use its service (social network), as it will not be intended for such cases. The approach outlined by the EDPB could lead to an interference with the freedom to conduct a business.

In the example of *Continuous prompting* in paragraph 28 is stated: *"The **Continuous prompting** dark pattern occurs when users are pushed to provide more personal data than*

*necessary for the processing purposes or to consent to another use of their data, by being repeatedly asked to provide additional data and offered arguments why they should provide it.“* A distinction should be made here between the unreasonable repetition of requests for consent and the reasonable reminder that consent can be given. In no provision does the GDPR prohibit seeking consent *per se*. Repeated requests would be contrary to the GDPR only if they would put the user under such disproportionate pressure to give the consent that the consent can no longer be considered free (see also paragraph 110).

In Paragraph 30 (*„To observe the principle of data minimisation, social media providers are required not to ask for additional data such as the phone number, when the data users already provided during the signup process are sufficient. For example, to ensure account security, enhanced authentication is possible without the phone number by simply sending a code to users' email accounts or by several other means.“*) we would like to point out that the possibility of higher account security, e.g. through two-factor authentication using a mobile phone number, is a common security practice. Therefore, this measure cannot be completely rejected, although there are alternative methods. Rather, it is important that the provision of a telephone number is not requested for purposes other than ensuring security.

In our view, the situation described in point 45 cannot always be considered as dark patterns. Whether the user is asked if it is his/her true choice, it should, to a certain extent, be left to the discretion of the social network provider concerned. We can imagine a number of cases where such a procedure will be appropriate - for example, analysis of users behaviour will show that in this particular case, users often click on the button by mistake. Then it makes sense to ask them in advance to confirm their choice. The same applies to the example 39 in paragraph 126.

In the case of the example given in paragraph 52, we do not agree that it is an example of dark patterns - Deceptive Snugness. According to the GDPR, the use of such approaches must be seen ***in the light of the purpose of the processing***. The purpose of data processing within the social network is to publish data among its users/all users of internet. It is then not possible to burden the provider for choosing such a solution that best suits to fulfilment of this purpose, especially in a situation where most users prefer this option. The principle of data minimization must be interpreted in the context of the purpose of the processing. We cannot therefore agree with the view expressed in paragraph 53: „*This is a **Deceptive Snugness** pattern, as it is not the option offering the highest level of data protection that is selected, and therefore activated, by default.*“. The purpose of the processing must always be taken into account.

On the contrary, we consider the defence against the "Dead End" expressed, for example, in paragraph 58, to be a very important principle.

In Paragraph 13 EDPB states: „*A privacy notice describes part of a processing in a vague and imprecise way, as in this sentence: “Your data might be used to improve our services”.“*

Although we generally agree with this view, we must point out that in practice it is often difficult to pre-determine examples of how data will be used in this way, as it is a never-ending process of service improvement and response to changes in environment and/or market practise. In reality, various minor adjustments and interface tests within the A / B testing are often performed within the social network.

The view expressed in paragraph 75: : „*For example, users should be able to exercise data subject rights via the platform's menu as well“*, should rather be a best practice recommendation. In particular, smaller social networks do not have such functionality (or do not have it as a complex tool) and rely on common requests sent by e-mail.

We do not consider the example in point 83 to be dark patterns. We generally consider it is beneficial for the user to be notified that the provider has taken corrective action. The provision of additional information should not in itself be considered as dark patterns unless it is intended to prevent the user from understanding the meaning of the message in question. In practice, it is common for the provider concerned to show that he is active and to minimize damage.

We do not believe that every social network should allow users to decide with whom they will share their information (see Paragraph 114). It is conceivable that smaller social networks in particular will be based on the principle of always sharing all information with all users. If the user is duly notified during registration, there is no reason to consider such approach defective.

We see the example in point 121 („*When users change a data protection setting, the principle of fairness also requires social media providers to inform users about other settings that are similar"*) as best practice rather than an obligation for the provider.

With regard to Example 40 in paragraph 128, we are not sure whether these will be dark patterns in all cases. The situation where it is necessary to click on an option to show other options is quite common in practice.

If the example of *non-users* is mentioned in paragraph 133, we would like to point out that this is a relatively complex problem, which covers a whole range of situations. From processing non-users' phone numbers provided by users in order to find a contact, through processing information about non-users in a private chat among two users, etc. In our opinion, this issue would rather deserve a separate detailed opinion.

With regard to the view set out in paragraph 150 (see also paragraph 154): *„The decision to permanently leave the social media platform is accompanied by the right to erasure in Article 17 (1) (a) GDPR. In this context the word "deletion" is used more often than erasure*.", we do not consider that the decision to terminate the service (the user's contractual relationship with the service provider) shall be accompanied by the right to erasure according Art. 17 of GDPR. We believe that this is much more the „normal" termination of the user's contractual relationship with the service provider, which induce consequences associated with the principle of storage limitation within the meaning of Article 5 e) GDPR.

While it is true that the termination of a service usually ends the right of the provider to process personal data obtained through consent (see paragraph 158 as well), in many cases the provider's other processing purpose may justify the retention of the data (or at least part of it) for a certain period in the archive. This may be for example a legitimate interest of provider to process some data for purpose a defence against legal claims by third parties potentially affected by the published content (e.g. in case of copyright infringement) or even directly a legal obligation (see for example Article 6 of Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online).

**We are grateful for the opportunity to provide our comments on the draft Guidelines.**

Prague, 2.5.2022

**JUDr. Vladan Rámiš, Ph.D.**
Chairman of the Committee
**Spolek pro ochranu osobních údajů**

**Mgr. Martin Cach**
Member of the Committee
**Spolek pro ochranu osobních údajů**