DMA Finland opinion on EDPB draft Guidelines 3/2022 on Dark Patterns in social media platform interfaces: How to recognize and avoid them

Data & Marketing Association Finland is giving the following comments on the above mentioned guidelines.

1. General comments on the guidelines

Dark Patterns is about finding the right balance between data usage and data protection. Indeed, by setting such a high standard of accountability, transparency and protection by design, the EDPB is pushing for strong data protection, necessary and proportionate use of data. This is understandable in the context of social media which tends to be high processing environment, including of sensitive data. However, this is not the case of every data processing context for data marketing purposes. We express our concern that applying these detailed guidelines will generate high costs to European SMEs to the benefit of major multinational companies who can afford the detailed assessments needed to reach such high standards of accountability.

A fundamental problem with the draft from our point of view is that any (broader) processing of personal data required by a social media service is easily seen as a breach of privacy. As if processing as little data as possible is the core goal. The benefits of data processing to the user or customer are hardly recognized. It seems that any presentation which promotes or visually supports processing of data in the context of social media and online targeted ad could become a Dark Pattern. The underlying message of these guidelines is that, either the options which minimize the processing of data must be highlighted or all options must be presented exactly the same way, which is in contradiction with the risk-based approach.

Many of the guideline examples are not in themselves contradictory, but the overall tone of the guidelines, which favors "neutral visual layouts - neutral texts - no innovative solutions, no temptation", is a concern.

The draft is far too heavy and long – 64 pages – with 176 numbered paragraphs. Also it is stated that the guidelines are meant for designers and users, but that the actual decisions of what kind of solutions are acceptable are made independently by the national authorities. However, in practice, the national authorities apply these EDPB guidelines as if they are legally binding and mandatory. These guidelines should not set principles, which will extend as such, to practices, outside of social media, which can be less risky. For example, if a small online shop has a broken link in a privacy notice to the DPA or promotes providing an email address to receive a newsletter, authorities should leverage the risk based approach and article 83 of the GDPR to make a balanced decision. This should not automatically be considered as “left in the dark” or “emotional steering”.

Consent is overemphasised in the draft as the legal basis for the processing of personal data, while contract (or legitimate interest) is hardly mentioned or recognized as a possible basis for processing in social media services.

The scope of the draft is limited solely to social media services and the processing of personal data in them. The draft walks through the life cycle of a service from signing up to exiting by use cases. However, it is likely that the guidelines will be applied to other types of services as well as interpretative material.

A positive feature in the guidelines is that there are good best practice listings in it, such as on page 22 for sign-up process. However, some of these listings are confusing because they can be enforced by consumer authorities only.

2. Detailed comments on the numbered paragraphs of the guidelines

Paragraph 26: Mandatory confirmation of reading the privacy information before gaining access to a social media platform.
Data protection and consumer protection laws as well as special legislation oblige service providers to inform their users of a huge set of different things. It is a common practice that when a user creates an account in a social media platform the user confirms that he or she has read the privacy information before gaining access to the platform as a mandatory step in the sign-in process. The draft states that this is not acceptable: *"when users are "required" to confirm that they have read the entire privacy policy and agree to the terms and conditions of the social media provider, including all processing operations, in order to create an account, this can qualify as forced consent to special conditions named there."* and *"Consent that is "bundled" with the acceptance of the terms and conditions of a social media provider does not qualify as "freely given"."* However, the draft does not give examples of *how* the data protection information should be presented to the user in an acceptable way.

ii. Withdrawal of consent (page 14)
The draft takes a very strict view on how withdrawing consent can be carried out in an acceptable way: - - *consent cannot be considered valid under the GDPR when consent is obtained through only one mouse-click, swipe or keystroke, but the withdrawal takes more steps, is more difficult to achieve or takes more time."* Counting and comparing the exact amount of individual mouse-clicks, swipes or seconds is not an appropriate method of validating consent and its withdrawal but it leads to a very mechanical interpretation of what is acceptable and what is not. Instead, the principles for interpretation should be laid out on a more general level concentrating on fair, transparent and moderate processes for the users of social media platforms.

Paragraphs 28-33 – Requesting a phone number for security purposes
In the examples of these paragraphs, requesting a phone number for security purposes is regarded as a Dark Pattern as a breach of the data minimizing principle because *"- - enhanced authentication is possible without the phone number by simply sending a code to users' email accounts or by several other means."* As well, according to Paragraph 33 a later request for a phone number if the user has previously refused to give it, is regarded as continuous prompting: *"However, this variation still constitutes a Continuous prompting dark pattern, as the social media provider disregards the fact that users previously refused to provide the phone number, and keeps asking for it."*
However, for example the National Cyber Security Centre of the Finnish Transport and

Communications Agency Traficom strongly recommends Multi-Factor Authentication – and the use of a phone number in the authentication process – as a security feature in online services that require logging in (https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/multi-factor-authentication-protects-your-user-accounts). We strongly agree with the Finnish authority in their interpretation as it protects the security of the users of on-line services. In this issue, according to our opinion information security weighs heavier than data minimization as a basic principle in data protection.

Paragraphs 37-38 – Request for a phone number to receive a link to a mobile application
Requesting a phone number when registering to a social media service is regarded as an "Misleading information" type of a Dark Pattern: *"Misleading information for a number of reasons: First of all, there are several ways for users to use an application, e. g. by scanning a QR code, using a link or by downloading the App from the store for applications. Second, these alternatives show that there is no mandatory reason for the social platform provider to ask for the users' phone number."* In our opinion, this interpretation is unreasonable and sets unfounded limits to the service design options of service providers.

Paragraphs 39- 44 – Emotional steering
"The manner in which the information is presented to users influences their emotional state in a way that is likely to lead them to act against their data protection interests." The examples of these paragraphs are naive and they underestimate the intelligence of the reader of the draft and of the users of various on-line services. They also express great reservations about various motivational linguistic expressions and prompts. For example the following promt is regarded as a Dark Pattern: *"Tell us about your amazing self! We can't wait, so come on right now and let us know!"* In our opinion, this interpretation limits in an unreasonable way the possibilities to develop the verbal design of social media services.

Paragraphs 81-91 – Communication practices in personal data breach notification context
These paragraphs cover various bad and inappropriate communication practices in data breach notification cases. As the scope of these guidelines is Dark Patterns in social media services and not personal data breaches, one may ask if these examples are in the right place at all. Should they be included in the Data Breach Notification guidelines instead?

Paragraphs 92-111 – Consent management
These paragraphs cover various examples of giving, informing of and refusing consent, such as ambiguous texts and repeated questions. For example a humoristic link to a baking recipe in a cookie banner is regarded as unacceptable (paragraphs 100-101) while *"- - users might think they just dismiss a funny message about cookies as a baked snack and not consider the technical meaning of the term "cookies…. wordplay based on "cookie" homonyms can make the bakery context outshine the data protection context."* We repeat our former opinion on underestimating the intelligence of social service platform users. In our mind it is important that service providers are allowed to use business models and language that is best suited to the target group of the social media service in question.