Freshfields Bruckhaus Deringer

Dark patterns: what data controllers should be aware of

Michael Schwaab,

April 19, 2022

The European Data Protection Board (EDPB) recently published its 'Guidelines 3/2022 on Dark patterns in social media platform interfaces' providing detailed guidance for all social media platforms on obtaining valid consent within the principles of the General Data Protection Regulation (GDPR). This guidance offers practical recommendations on how to assess and avoid so-called 'dark patterns' in social media interfaces that infringe GDPR.

The EDPB's guidance provides a non-exhaustive list of examples of what controllers must watch out for when obtaining valid consent from users. While it is primarily aimed at social media platforms, the examples have much wider relevance for other industry sectors. For example, cookie consent tools on web pages, newsletter registrations or interfaces for creating accounts typically use similar techniques to achieve the highest possible conversion rate. The EDPB states that the guidelines are 'also suitable for increasing the awareness of users regarding their rights, and the risks possibly coming from sharing too many data or sharing their data in an uncontrolled way.'

Furthermore, the German *Datenschutzkonferenz* (the body of independent federal and state German data protection supervisory authorities) recently published a short assessment on the conformity of Facebook Fanpages (only available in German) that included an in-depth examination of the (dark) patterns of the provided consent-banner.

Dark patterns to be on the lookout for

Dark patterns are interfaces and user experiences that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data. The EDPB identifies the following categories of dark patterns:

- **Overloading.** By confronting the user with a large amount of requests, information, options or possibilities, the users are pushed to share more data. With this dark pattern, users tend to be exhausted from having to refuse the request each time they visit the website or application and are therefore likely to end up giving in and submitting more data.
- **Skipping.** Designing the interface to create a deceptive snugness or distraction will make the users forget or not think about all or some of the data they are going to share. In particular, if data settings are preselected or not changeable on the first layer, such dark patterns may nudge individuals to keep a preselected option or obstruct them to click through all the sub-layers and change the settings.
- **Stirring.** By using patterns, wordings or visuals, users are 'emotionally steered' in a way that conveys information to users in either a highly positive or negative. Such dark patterns may lead users against their data protection interests.
- **Hindering.** By obstructing or blocking users in their process of becoming informed or managing their data and making the action difficult or even impossible to achieve, users are likely to be discouraged by these dark patterns from taking control of their data.
- **Fickle.** By using an inconsistent and unclear interface, users will find it difficult to navigate the different data protection control tools and may fail to fully understand the purpose of the processing. Users are likely to be confused by such dark patterns and therefore likely unable to fully understand how their data is processed and how to exercise control over it.
- **Left in the dark.** By designing the user interface in a way that hides information or data protection control tools, users are likely to be left unsure of how their data is processed and what kind of control they might have. Such dark patterns leave the average user in the dark and therefore unable to exercise their rights.

Not all dark patterns will render consent invalid

The usage of dark patterns can lead to the invalidity of obtained consents. The EDPB takes a rather strict stance in their guidance and considers that almost every form of guided user experience may entail the risk of dark patterns. This has a significant impact on all those aiming for a high conversion rate while trying to obtain consent. However, the guidance itself does not specifically state whether the provided examples will definitively lead to the invalidity of the provided consent, but rather that they entail a risk. It is therefore necessary to look at the consent process on a

case-by-case basis to determine whether it is necessary to provide additional information or refrain from certain practices.

The EDPB also provides some recommendations on mitigating these risks:

- **Usability of privacy policy.** To increase the usability for users, the EDPB recommends the implementation of shortcuts to the data protection settings, clearly stating the company's contact information, as well as the specific identity of the supervisory authority, with a link to its website and clearly structuring the privacy policy divided by headings and subheadings.
- **Avoid continuous prompting.** In order to avoid user fatigue, pop-ups should not be used excessively.
- **Reasoned preselection.** The departure from less privacy-friendly settings by default must be justified. In the best case, the interface should not anticipate the decision of the users by preselecting options.
- **Availability of privacy settings.** An easily accessible page should be provided, from where all data protection related actions and information is accessible. Those settings should be available cross-device.
- **Clear Language.** Coherent language should be used, definitions should be provided where necessary, and examples should be given. Changes in the privacy policy should be comprehensible at any time.

Controllers remain accountable and responsible for ensuring that they are GDPR-compliant at all times. Accountability can be provided by the user interface design itself as proof of the controller's compliance with the GDPR to demonstrate that the users have read and considered data protection information, have freely given their consent, have easily exercised their rights, etc. Given the potential for dark patterns to be used on nearly all other kinds of website, businesses with an online presence should be aware of the risks and mitigation strategies, and monitor developments closely.