60 YEARS YOUNG YEARS STRONG

BEUC The European Consumer Organisation

The Consumer Voice in Europe

BEUC COMMENTS ON THE EDPB GUIDELINES ON DARK PATTERNS IN SOCIAL MEDIA PLATFORM INTERFACES

Contact: Wolfgang Schmitt – digital@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2022-043 - 02/05/2022

Why it matters to consumers

Millions of consumers use social media platforms every day and are faced with 'dark patterns' in the user interface design of these platforms. These interfaces are often designed to deceive consumers so that they take decisions that serve companies' commercial interests and allow them to exploit consumers' privacy and personal data. The EU General Data Protection Regulation must be applied effectively to protect consumers against such practices, for example, by ensuring that consumers' are not nudged, pressured or tricked into giving consent to the use of their personal data, and guaranteeing that personal data is processed in a fair and transparent manner.

Introduction

Consumers use social media platforms every day. Through these platforms, social media companies are collecting a vast amount of personal data which allows them to monitor and analyse practically every move and click social media users make.

Companies rely on users' consent to collect a vast amount of data. Consent is very often the door-opener into consumers' private lives. It is therefore of utmost importance for the protection of consumers that the General Data Protection Regulations (GDPR) rules on consent are effectively applied and respected. This will help ensure consumers can make a freely given, informed, unambiguous and specific choice.

BEUC welcomes the EDPB guidelines on dark patterns in social media platform interfaces. These provide valuable guidance on the application of the GDPR regarding these practices, and useful practical examples of dark patterns that are not in line with the GDPR, including ways to hinder, emotionally stir, and even obstruct a user's decision to leave social media accounts. These guidelines reinforce the key role of the GDPR principles of fairness (Art 5.1a GDPR) and data protection by design (Art 25.1 GDPR), which are particularly important in the context of 'dark patterns'.

We would also like to underline that 'dark patterns' are practices that are not only highly relevant for personal data protection but sit at the intersection between several fields of law in particular consumer law (see "Dark Patterns And The EU Consumer Law Acquis" by BEUC[1]), digital market and data protection law. The Digital Markets Act and Digital Services Act also contain specific provisions prohibiting these types of practices and they are also addressed in other instruments regulating the digital sphere which are currently under discussion, such as the Data Act. It is important that all the existing rules are applied in a coherent and complementary manner and that DPAs and other relevant enforcement authorities at EU and national level cooperate closely on this matter, specifically by alerting one another when they identify practices which may break the law.

[1] BEUC, "Dark Patterns" And The EU Consumer Law Acquis, 7.2.2022, https://www.beuc.eu/publications/beuc-x-2022-013_dark_patters_paper.pdf

1. Scope of the guidelines

The guidelines provide recommendations and guidance on how to collect valid consent on social media platforms over the full life cycle of a social media account. BEUC supports the approach taken by the EDPB, analysing the different stages of a life cycle of a social media account and the challenges present at every stage. The guidelines directly address examples of dark patterns that consumers face every day, and which strongly affect their behaviour.

Nevertheless, we must underline that consumers also face dark patterns outside of social media platforms, most prominently, in cookie banners throughout the internet. Social media companies often also profit from data collected on third-party services via cookies. BEUC would therefore recommend the addition of some examples of dark patterns in cookie banners and the extension of the scope of the guidelines to cover dark patterns that are not limited to social media platforms.

2. Opening a social media account

Opening a social media account involves making important decisions. Consumers typically click through the process quickly. They do not want to spend much time on it, and they cannot afford to read complicated information and terms of use, which are unclear and lead to more questions than answers. Consumers usually choose the fastest path through the sign-up process. They stick to the default settings or the options which are recommended by the service provider. As a result, data protection by design and by default is a central principle to protect data subjects' rights and freedoms in this context, as underlined in the guidelines.

We would like to underline the following examples of dark patterns linked to the process of opening a social media account, which illustrate several crucial points for consumers from a GDPR perspective.

2.1. More steps to enact privacy (hindering - Longer than necessary)

The dark pattern example in paragraph 45 of the guidelines describes a sign-up process that requires more steps to activate the 'data protective' options than the 'data invasive' options. In practice, this is likely to discourage consumers from activating the 'data protective' controls. BEUC fully supports the EDPB's interpretation that a sign-up process which is designed in this way is incompatible with a freely-given consent and the privacy-by-design and by-default principles.

Furthermore, this example leads to the very relevant general legal question of whether consumers must be able to refuse consent as easy as they can give consent. While Article 7 (3) phrase 4 GDPR and the guidelines in paragraph 26 answer this clearly in relation to the withdrawal of consent, the GDPR does not provide information about formal requirements for refusing consent. Nevertheless, we are of the opinion that refusing consent must be as easy as it is to give it, which derives from the criteria that consent must be freely given according to Art 4 Nr 11 GDPR. As the EDPB already stated in their guidelines on consent: "any element of inappropriate pressure or influence upon a data subject which prevents a data subject from exercising their free will, shall render the consent invalid"[2]. We would consider a design pattern that discourages consumers from choosing a more privacy-friendly setting as one such example. Additionally, such a pattern

[2] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 4.5.2020, para 14).

will also inevitably conflict with the privacy-by-design and by-default principles. According to the privacy-by-design principle, data controllers must implement appropriate technical and organisational measures that are designed to implement data-protection principles, such as data minimisation. A signing-up process that, in the click of one button, sets several, privacy-invasive parameters, yet requires more clicks to achieve a privacy-friendly result, is clearly not using appropriate technical and organisational measures to implement data-protection principles and is therefore breaking the law. Also, not setting the most privacy-friendly options as the default conflicts with the privacy-by-default principle. To avoid further uncertainty, BEUC would welcome the guidelines clearly stating that refusing consent should be as easy as giving consent.

2.2. Generating emotional reaction (stirring – Emotional steering and Hidden in Plain Sight)

Consumers often face situations online where they have the feeling that either the content or the interface of a service managed to compel them to click on or decide something that they did not want.

Emotional steering refers to dark patterns that try to influence the behaviour of consumers by steering their emotions via words and visuals. This influence can already be exerted at a supposedly low threshold level, like the examples mentioned in the guidelines (see paragraph 39ff and 47ff). Yet, the consent obtained via emotional steering often involves deep intrusions into consumers' privacy. As previously mentioned, and the guidelines point out**,** consumers want to complete the sign-up process "in a rush" in order to use the platform. They are therefore particularly vulnerable to influence at this stage.

It is important to clearly state that the emotion factor has a strong influence on the legitimacy of consent. It is an important element to assess whether the consent was freely given, or whether an inappropriate pressure or influence prevented the data subjects from exercising their free will.

Hidden in Plain Sight refers to dark patterns that make use of visual means such as a biased presentation of information and options for consumers (see paragraph 47 ff). Such practices are trying by design to nudge consumers to choose a more privacy-invasive option. The guidelines are correctly stating that those patterns are in conflict with the principles of fairness and transparency (Art 5.1a GDPR). BEUC sees an urgent need to fight such deceptive patterns and therefore welcomes the clarity of the guideline under point 4.3.2 and the examples put forward (example 8, 34, 40 and 48), which clearly state how these practices breach the GDPR.

3. Staying informed on social media

We agree that the principle of transparency is very closely linked to the principle of fair processing of personal data, as the guidelines state. Therefore, it is very important for consumers to receive information that is comprehensible to them. This includes information that is presented to consumers across different layers as described in the use case 2a of the guidelines. But as the EDPB rightfully states in paragraph 61: too much irrelevant or confusing information can obscure important content or reduce the likelihood of finding it. Hence, the right balance between content and comprehensible presentation is crucial.

3.1. Left in the dark and lacking hierarchy

The privacy notice is the one source of information where consumers can find out what companies do with their personal data. In the dark pattern category named 'left in the

dark' (paragraph 5), the guidelines refer to content and interfaces that are designed to hide information or data protection control tools or that leave users unsure about how their data is processed. We agree that a layered privacy notice can help create the right balance between content and comprehensible presentation. Nevertheless, social media companies should not misuse the layered approach to hide information in deeper layers or to send consumers on a 'privacy journey' by adding links to previous or irrelevant layers.

It is important that information about the purpose(s) of processing is not split across different layers and that the structure and hierarchy is presented in a comprehensible way, so consumers can easily understand what information applies to which purpose. Secondly, the dark pattern 'lacking hierarchy' underlines the importance for consumers that the information presented to them follows an intelligible structure and hierarchy (see paragraph 66ff). Hence, consumers should not be left more confused after trying to find out more about a specific data processing by, for example, searching for additional information on deeper layers.

Finally, the number of layers of information should be kept to the minimum possible. Two layers, or in exceptional cases a maximum of three layers, should be sufficient to present all information. Examples 13 and 14 put forward by the EDPB in the guidelines provide a good illustration of how to address these issues and ensure information is presented in a way which respects the requirements of the GDPR.

4. Leaving a social media platform

4.1. Pausing the account and/or erasure of all personal data

Registering on a social media platform must not be a lifelong engagement for consumers. Many consumers reach the point where they are not interested in using a certain service anymore. Social media companies must respect this decision and consumers must be able to effectively exercise their right to erasure.

Unfortunately, consumers often face hurdles to get to the point where the social media platform provider finally proceeds with the deletion of the account. By imposing cooling off periods and by using features like pausing/deactivating of accounts and other forms of dark patterns, providers often try to delay or avoid the deletion of the account. For consumers, this means that stopping to use a service is often much more complicated than signing up for it. In many cases, consumers are unable to navigate to the 'erase my account' process without looking up a step-by-step guide.

Furthermore, we consider the 'pause' and 'deactivate' functions to be misleading by design. Not only do consumers not know how their data will be processed during these periods, but these features are also distracting them from their initial wish to delete their data.

Similarly, cooling off periods seem to ignore that data controllers must execute erasure requests without undue delay.

The examples given in the guidelines reflect the experience of consumers and BEUC and its members on this issue (see the report "You can log out, but you can never leave. How Amazon manipulates consumers to keep them subscribed to Amazon Prime" by the Norwegian Consumer Council[3]).

[3] Norwegian Consumer Council, You can log out, but you can never leave. How Amazon manipulates consumers to keep them subscribed to Amazon Prime, 14.1.2021, https://fil.forbrukerradet.no/wp-content/uploads/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf

BEUC fully supports the EDPB interpretation that these types of dark patterns breach the GDPR by preventing, deterring, or making it more difficult for data subjects to exercise their right to erasure.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.