Guidelines 03/2022 on

Deceptive design patterns in social media platform interfaces:

how to recognise and avoid them

Version 2.0

Adopted on 14 February 2023

Version history

Version 2.0	14 February 2023	Adoption of the Guidelines after public consultation
Version 1.0	14 March 2022	Adoption of the Guidelines for public consultation

EXECUTIVE SUMMARY

These Guidelines offer practical recommendations to social media providers as controllers of social media, designers and users of social media platforms on how to assess and avoid so-called "deceptive design patterns" in social media interfaces that infringe on GDPR requirements. To this end, the EDPB recommends that controllers make use of interdisciplinary teams, consisting, among others, of designers, data protection officers and decision-makers. It is important to note that the list of deceptive design patterns and best practices, as well as the use cases, are not exhaustive. Social media providers remain responsible and accountable for ensuring the GDPR compliance of their platforms.

Deceptive design patterns in social media platform interfaces

In the context of these Guidelines, "deceptive design patterns" are considered as interfaces and user journeys implemented on social media platforms that attempt to influence users into making unintended, unwilling and potentially harmful decisions, often toward a decision that is against the users' best interests and in favour of the social media platforms interests, regarding the processing of their personal data. Deceptive design patterns aim to influence users' behaviour and can hinder their ability to effectively protect their personal data and make conscious choices. Data protection authorities are responsible for sanctioning the use of deceptive design patterns if these breach GDPR requirements. The deceptive design patterns addressed within these Guidelines can be divided into the following categories:

- ***Overloading*** means users are confronted with an avalanche/large quantity of requests, information, options or possibilities in order to prompt them to share more data or unintentionally allow personal data processing against the expectations of the data subject.
  The following three deceptive design pattern types fall into this category: ***Continuous prompting***, ***Privacy Maze*** and ***Too Many Options***

- ***Skipping*** means designing the interface or user journey in a way that users forget or do not think about all or some of the data protection aspects.
  The following two deceptive design pattern types fall into this category: ***Deceptive Snugness*** and ***Look over there***

- ***Stirring*** affects the choice users would make by appealing to their emotions or using visual nudges.
  The following two deceptive design pattern types fall into this category: ***Emotional Steering*** and ***Hidden in plain sight***

- ***Obstructing*** means hindering or blocking users in their process of becoming informed or managing their data by making the action hard or impossible to achieve.
  The following three deceptive design pattern types fall into this category: ***Dead end***, ***Longer than necessary*** and ***Misleading action***

- ***Fickle*** means the design of the interface is inconsistent and not clear, making it hard for the user to navigate the different data protection control tools and to understand the purpose of the processing.
  The following four deceptive design pattern types fall into this category: ***Lacking hierarchy, Decontextualising, Inconsistent Interface*** and ***Language Discontinuity***

- ***Left in the dark*** means an interface is designed in a way to hide information or data protection control tools or to leave users unsure of how their data is processed and what kind of control they might have over it regarding the exercise of their rights.
  The following two deceptive design pattern types fall into this category: ***Conflicting information*** and ***Ambiguous wording or information***

Relevant GDPR provisions for deceptive design pattern assessments

Regarding the data protection compliance of user interfaces of online applications within the social media sector, the data protection principles applicable are set out within Article 5 GDPR. The principle of fair processing laid down in Article 5 (1) (a) GDPR serves as a starting point to assess whether a design pattern actually constitutes a "deceptive design pattern". Further principles playing a role in this assessment are those of transparency, data minimisation and accountability under Article 5 (1) (a), (c) and (2) GDPR, as well as, in some cases, purpose limitation under Article 5 (1) (b) GDPR. In other cases, the legal assessment is also based on conditions of consent under Articles 4 (11) and 7 GDPR or other specific obligations, such as Article 12 GDPR. Evidently, in the context of data subject rights, the third chapter of the GDPR also needs to be taken into account. Finally, the requirements of data protection by design and default under Article 25 GDPR play a vital role, as applying them before launching an interface design would help social media providers avoid deceptive design patterns in the first place.

Examples of deceptive design patterns in use cases of the life cycle of a social media account

The GDPR's provisions apply to the entire course of personal data processing as part of the operation of social media platforms, i.e. to the entire life cycle of a user account. The EDPB gives concrete examples of deceptive design pattern types for the following different use cases within this life cycle: the sign-up, i.e. registration process; the information use cases concerning the privacy notice, joint controllership and data breach communications; consent and data protection management; exercise of data subject rights during social media use; and, finally, closing a social media account. Connections to GDPR provisions are explained in two ways: firstly, each use case explains in more detail which of the above-mentioned GDPR provisions are particularly relevant to it. Secondly, the paragraphs surrounding the deceptive design pattern examples explain how these infringe on the GDPR.

Best practice recommendations

In addition to the examples of deceptive design patterns, the Guidelines also present best practices at the end of each use case, as well as in Annex II to these Guidelines. These contain specific recommendations for designing user interfaces that facilitate the effective implementation of the GDPR.

Checklist of deceptive design pattern categories

A checklist of deceptive design pattern categories can be found in Annex I to these Guidelines. It provides an overview of the abovementioned categories and the deceptive design pattern types, along with a list of the examples for each pattern that are mentioned in the use cases. Some readers may find it useful to use the checklist as a starting point to discover these Guidelines.

Table of contents

The European Data Protection Board

Having regard to Article 70 and (1e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,[1]

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES

1 SCOPE

1. The aim of these Guidelines is to provide recommendations and guidance for the design of the interfaces of social media platforms. For the purposes of these Guidelines, social media are understood as online platforms that enable the development of networks and communities of users, among which information and content is shared.[2] The Guidelines can be used either at the conception phase of a user interface, to avoid the implementation of deceptive design patterns[3] from the start, or on an existing service, to evaluate the compliance of its interface. They are aimed at social media providers as controllers of social media, who have the responsibility for the design and operation of social media platforms. In this regard, the Guidelines aim to recall the obligations coming from the GDPR, with special reference to the principles of lawfulness, fairness, transparency, purpose limitation and data minimisation in the design of user-interfaces and content presentation of their web services and apps. The aforementioned principles have to be implemented in a substantial way and, from a technical perspective, they constitute requirements for the design of software and services, including user interfaces. An in-depth study is made on the GDPR's requirement when applied to user interfaces and content presentation, and it is going to be clarified what should be considered a "deceptive design pattern", a way of designing and presenting content which substantially violates those requirements, while still pretending to formally comply. These 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. These Guidelines also aim to educate users to recognise "deceptive design patterns" (as defined in the following), and how to face them to protect their privacy in a conscious way. As part of the analysis, the life cycle of a social media account was examined on the basis of five use cases: "Opening a social media account" (use case 1), "Staying informed on social media" (use case 2), "Staying protected on social media" (use case 3), "Staying right on social media:

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".

[2] Definition identical to EDPB Guidelines 08/2020 on Targeting of social media users, para. 1, see footnote 1 there for more detailed description; available at https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.

[3] For version 2.0 of these Guidelines, the EDPB is using the more inclusive and descriptive term "deceptive design pattern" instead of "dark pattern".

data subject rights" (use case 4) and "So long and farewell: leaving a social media account" (use case 5).

2. In these Guidelines, the term "user interface" corresponds to the means for people to interact with social media platforms. The document focuses on graphical user interfaces (e.g. used for computer and smartphone interfaces), but some of the observations made may also apply to voice-controlled interfaces (e.g. used for smart speakers) or gesture-based interfaces (e.g. used in virtual reality). The term "user journey" corresponds to the series of actions or steps for users to perform in order to reach their goal which, on social networks, can be things such as browsing their feed, sharing a post, setting their preferences, etc. The term "user experience" corresponds to the overall experience users have with social media platforms, which includes the perceived utility, ease of use and efficiency of interacting with it. User interface design and user experience design have been evolving continuously over the last decade. More recently, they have settled for ubiquitous, customised and so-called seamless user interactions and experiences: the perfect interface should be highly personalised, easy to use and multimodal.[4] Even though those trends might increase the ease of use of digital services, they can be used in such a way that they primarily promote user behaviours that run against the spirit of the GDPR.[5] This is especially relevant in the context of the attention economy, where user attention is considered a commodity. In those cases, the legally permissible limits of the GDPR may be exceeded and the interface design and user experience design leading to such cases are described below as "deceptive design patterns".

3. In the context of these Guidelines, "deceptive design patterns" are considered interfaces and user journeys implemented on social media platforms that aim to influence users into making unintended, respectively unwilling, and/or potentially harmful decisions, often toward an option that is against the users' best interests and in favour of the social media platforms interest, with regard to their personal data. Deceptive design patterns aim to influence users' behaviours, generally relying on cognitive biases, and can hinder their ability "to effectively protect their personal data and make conscious choices"[6], for example by making them unable "to give an informed and freely given consent".[7] This can be exploited in several aspects of the design, such as interfaces' colour choices and placement of the content. Conversely, by providing incentives and user-friendly designs, the realisation of data protection regulations can be supported.

4. Deceptive design patterns do not necessarily only lead to a violation of data protection regulations. Deceptive design patterns can, for example, also violate consumer protection regulations. The boundaries between infringements enforceable by data protection authorities and those enforceable by national consumer protection, competition or other authorities, can overlap.[8] Under the GDPR,

[4] For more details see CNIL, IP Report No. 6: Shaping Choices in the Digital World, 2019. p. 9 https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

[5] CNIL, Shaping Choices in the Digital World, 2019. p. 10.

[6] CNIL, Shaping Choices in the Digital World, 2019. p. 27.

[7] See Norwegian Consumer Council, *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*, p. 10 https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf, but also CNIL, Shaping Choices in the Digital World, p. 30, 31.

[8] In this regard, Article 25 (2) of the Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), clarifies that the prohibition of deceiving or manipulating designs of online interfaces under its Article 25 (1) shall not apply to practices covered by Directive 2005/29/EC (Directive concerning unfair business-to-consumer commercial practices directive, UCPD) or the

data protection authorities are responsible for sanctioning the use of deceptive design patterns if they actually violate data protection standards and thus the GDPR. Breaches of GDPR requirements need to be assessed on a case-by-case basis. Only deceptive design patterns that might fall within this regulatory mandate are covered by these Guidelines. For this reason, in addition to examples of deceptive design patterns, the Guidelines also present best practices that can be used to design user interfaces which facilitate the effective implementation of the GDPR. Such best practices can offer a first step towards a standardised way for users to effectively control their data and exercise their rights.

5. The deceptive design patterns[9] addressed within these Guidelines result from an interdisciplinary analysis of existing interfaces and can be divided into the following categories:

Overloading: users are confronted with an avalanche/ large quantity of requests, information, options or possibilities in order to prompt them to share more data or unintentionally allow personal data processing against the expectations of data subject.

Skipping: designing the interface or user journey in a way that the users forget or do not think about all or some of the data protection aspects.

Stirring: affects the choice users would make by appealing to their emotions or using visual nudges.

Obstructing: an obstruction or blocking of users in their process of getting informed or managing their data by making the action hard or impossible to achieve.

Fickle: the design of the interface is inconsistent and not clear, making it hard for users to navigate the different data protection control tools and to understand the purpose of the processing.

Left in the dark: an interface is designed in a way to hide information or data protection control tools or to leave users unsure of how their data is processed and what kind of control they might have over it regarding the exercise of their rights.

6. In addition to regrouping deceptive design patterns in these categories according to their effects on users' behaviour, these patterns can also be divided into content-based and interface-based patterns to more specifically address aspects of the user interface or user journey. Content-based patterns refer to the actual content and therefore also to the wording and context of the sentences and information components. In addition, however, there are also components that have a direct influence on the perception of these factors. These interface-based patterns are related to the ways of displaying the content, navigating through it or interacting with it.

7. It is essential to keep in mind that deceptive design patterns raise additional concerns regarding potential impact on children,[10] registering with the social media platform, and also other vulnerable groups of people such as the elderly, persons who are visually impaired, or not as digitally literate as or others. Vulnerable groups such as elderly users are often not only less capable to identify manipulative design practices, but also less aware that their digital behaviour is subject to influence. The GDPR requires additional safeguards when the processing is about children's personal data, as the latter may be less aware of the risks and consequences concerned their rights to the processing.[11]

GDPR. Also, EU Commission Notice (2021/C 526/01) offers Guidance on the interpretation and application of the UCPD, including on "dark patterns" in its Section 4.2.7.

[9] Categories of deceptive design patterns and types of deceptive design patterns within these categories will be displayed in ***bold and italics*** in the text of the Guidelines. A detailed overview is provided in the Annex.

[10] See also Recital 81, phrase 4, of Regulation (EU) 2022/2065 (Digital Services Act).

[11] GDPR, Recital 38.

Recital 58 explicitly states that where processing is addressed to a child, any information should be given in a clear and plain language that children can easily understand. In addition, the GDPR explicitly includes the processing of individuals' data, particularly those of children, to be among the situations where the risk to the rights and freedoms of individuals of varying likelihood and severity, may result from data processing that could lead to physical, material or non-material damage.[12]

8. Keeping the above in mind, it should be understood that deceptive design patterns are not unique to social media platforms. Strong opinions on this issue were voiced during the public consultation of these Guidelines. Interfaces are present in many other instances where users interact with products and services based on or related with data processing operations. These may include websites and cookie banners,[13] online shops, video games, mobile applications and micropayments etc. Although the deceptive design patterns described below may not be present in the exact same form, their variations may still infringe upon the rights of data subjects or consumers. Nevertheless, these Guidelines focus solely on deceptive design patterns in social media platforms, as influence of these platforms on daily life of people and nations is constantly growing, which has been made clear in previous EDPB documents.[14]

2 PRINCIPLES APPLICABLE – WHAT TO KEEP IN MIND?

9. Regarding the data protection compliance of user interfaces of online applications within the social media sector, the data protection principles applicable are set out within Article 5 GDPR. The principle of fair processing laid down in Article 5 (1) (a) GDPR is a starting point for an assessment of existence of deceptive design patterns. As the EDPB already stated, fairness is an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject.[15] If the interface has insufficient or misleading information for users and fulfils the characteristics of deceptive design patterns, it can be classified as unfair processing. The fairness principle has an umbrella function and all deceptive design patterns would not comply with it irrespectively of compliance with other data protection principles.

10. Besides this fundamental provision of fairness of processing, the principles of accountability, transparency and the obligation of data protection by design stated in Article 25 GDPR are also relevant regarding design framework and deceptive design patterns could infringe those provisions. However, it is also possible that the legal assessment of deceptive design patterns can be based on the elements

[12] GDPR, Recital 75; see also EDPB Guidelines 8/2020 on targeting of social media users, para. 16 https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.

[13] Caused by a series of complaints received from NOYB, an EDPB Taskforce has exchanged views on a number of design elements in cookie banners. The common denominator agreed by the SAs in their interpretation of the applicable multi-layered legal framework has been summarized in a "Report of the work undertaken by the Cookie Banner Taskforce" of 17 January 2023, available at https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf.

[14] EDPB Guidelines 8/2020 on the targeting of social media users, Statement 2/2019 on the use of personal data in the course of political campaigns https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-22019-use-personal-data-course-political_en.

[15] EDPB Guidelines 4/20219 on Article 25 Data Protection by Design and by Default, version 2.0, adopted on 20 October 2020, p. 16; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

on general definitions such as Article 4 (11) GDPR, the definition of consent or other specific obligations such as Article 12 GDPR. Article 12 (1) phrase 1 GDPR requires controllers to take appropriate measures to provide any communication related to data subject rights, as well as any information, in a concise, transparent, intelligible and easily accessible form, using clear and plain language. As Recital 39 phrase 3 on the principle of transparency shows, this requirement is not, however, limited to data protection notices[16] or data subject rights,[17] but rather applies to any information and communication relating to the processing of personal data. Phrase 5 of the Recital also clarifies that data subjects should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

11. For the design of user interfaces of online applications, it is also important to take into account the principle of purpose limitation under Article 5 (1) (b) GDPR, as well as the principle of data minimisation under Article 5 (1) (c) GDPR. In any case, to ensure data protection compliance, controllers are well-advised to double-check compliance with all data protection principles under the GDPR.

2.1 Accountability

12. The accountability principle has to be reflected in every user interface design.

13. Article 5 (2) GDPR states that a controller shall be responsible for, and be able to demonstrate compliance with the GDPR principles which are described in Article 5 (1) GDPR. Therefore this principle is closely linked to the relevant principles mentioned above. Accountability can be provided by elements that provide proof of the social media provider's compliance with the GDPR. The user interface and user journey can be used as a documentation tool to demonstrate that users, during their actions on the social media platform, have read and taken into account data protection information, have freely given their consent, have easily exercised their rights, etc. Qualitative and quantitative user research methods, such as A/B testing, eye tracking or user interviews, their results and their analysis can also be used to support demonstration of compliance. It is important to note that such research methods often also involve processing of personal data, which therefore needs to be in line with the GDPR. If, for example, users have to tick a box or click on one of several data protection options, screenshots of the interfaces can serve to show the users' pathway through the data protection information and explain how users are making an informed decision. Results of user research made on this interface would bring additional elements detailing why the interface is optimal in reaching an information goal.

14. In the area of user interfaces, such documentary elements can be found in the disclosure of certain agreements and, above all, when evidence, for example of giving consent or a confirmation of reading, is obtained.

2.2 Transparency

15. The transparency principle in Article 5 (1) (a) GDPR has a large overlap with the area of general accountability. Even though controllers have to protect certain sensitive business information towards third parties, making documentation on processing accessible or recordable could help provide accountability: Confirmation of reading can be obtained, for example, for a text which the controller must make available in accordance with the principle of transparency. This can always serve at the same time to ensure transparency towards data subjects.

[16] Addressed in part 3.2. – use case 2a of these Guidelines.
[17] Addressed in use cases 4 and 5, i.e. parts 3.4 and 3.5 of these Guidelines.

16. All the data protection principles set out in Article 5 GDPR are specified further in the GDPR. Article 5 (1) (a) GDPR stipulates that personal data shall be processed in a transparent manner in relation to the data subject. The Guidelines on Transparency specify the elements of transparency as laid down by Article 12 GDPR, i. e. the need to provide the information in a "concise, transparent, intelligible and easily accessible form, using clear and plain language".[18] These Guidelines also provide guidance on how to fulfil the information obligations under Articles 13 and 14 GDPR regarding social media providers.

17. In addition, the text of the data protection principles of Article 5 (1) (a) GDPR and other special legal provisions within the Regulation contain many more details of the principle of transparency, which are linked to specific legal principles, such as the special transparency requirements in Article 7 GDPR for obtaining consent.

2.3 Data protection by design and default

18. Article 25 (1) GDPR specifies that controllers shall implement appropriate technical and organisational measures, which are designed to implement data-protection principles, whereas Article 25 (2) GDPR clarifies that such measures shall also be implemented for ensuring that, by default, only personal data which are necessary for each specific processing purpose are processed. In the context of the Guidelines 04/2019 on Article 25 Data Protection by Design and by Default, there are some key elements that controllers and processors have to take into account when implementing data protection by design regarding a social media platform. One of them is that with regard to the principle of fairness, the data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design.[19] The Guidelines identify elements of the principles for Data Protection by Default and Data Protection by Design, among other things, which become even more relevant with regard to deceptive design patterns:[20]

- Autonomy – Data subjects should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as autonomy over the scope and conditions of that use or processing.
- Interaction – Data subjects must be able to communicate and exercise their rights in respect of the personal data processed by the controller.
- Expectation – Processing should correspond with data subjects' reasonable expectations.
- Consumer choice – The controllers should not "lock in" their users in an unfair manner. Whenever a service processing personal data is proprietary, it may create a lock-in to the service, which may not be fair, if it impairs the data subjects' possibility to exercise their right of data portability in accordance with Article 20 GDPR.
- Power balance – Power balance should be a key objective of the controller-data subject relationship. Power imbalances should be avoided. When this is not possible, they should be recognised and accounted for with suitable countermeasures.
- No deception – Data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design.

[18] Article 29 Working Party Guidelines on transparency under Regulation 2016/679, endorsed by the EDPB https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.
[19] See Guidelines 04/20219 on Article 25 Data Protection by Design and by Default, p. 18, para. 70.
[20] Excerpt - for the full list, see Guidelines on Article 25 Data Protection by Design and by Default, para. 70.

- Truthful – the controllers must make available information about how they process personal data, should act as they declare they will and not mislead data subjects.

19. Compliance with Data Protection by Default and Data Protection by Design is important when assessing deceptive design patterns, as it would result in avoiding them in the first place. Indeed, confronting one's service and associated interfaces to the elements comprising Data Protection by Default and by Design principles, such as the ones mentioned above, will help identify aspects of the service that would constitute a deceptive design pattern before launching the service. For example, if data protection information is provided without following the principle "No deception", then it is likely to constitute a ***Hidden in Plain Sight*** or ***Emotional Steering*** deceptive design pattern that will both be further developed in use case 1.

3 THE LIFE CYCLE OF A SOCIAL MEDIA ACCOUNT: PUTTING THE PRINCIPLES INTO PRACTICE

20. The GDPR applies to the entire course of personal data processing by automated means.[21] In the case of processing of personal data as part of the operation of social media platforms, this leads to the application of the GDPR and its principles to the entire life cycle of a user account.

3.1 Opening a social media account

Use case 1: Registering an account

a. Description of the context

21. The first step users need to take in order to have access to a social media platform is signing up by creating an account. As part of this registration process, users are asked to provide their personal data, such as first and last name, email address or sometimes phone number. Users need to be informed about the processing of their personal data and they are usually asked to confirm that they have read the privacy notice and agree to the terms of use of the social media platform. This information needs to be provided in a clear and plain language, so that users are in a position to easily understand it and knowingly agree.

22. In this initial stage of the sign-up process, users should understand what exactly they sign up for, in the sense that the object of the agreement between the social media platform and users should be described as clearly and plainly as possible.

23. Therefore, data protection by design must be taken into account by social media providers in an effective manner to protect data subjects' rights and freedoms.[22]

b. Relevant legal provisions

24. Social media providers need to make sure that they implement the principles under Article 5 GDPR properly when designing their interfaces. While transparency towards the data subjects is always essential, this is especially the case at the stage of creating an account with a social media platform. Due to their position as controller or processor, social media platforms should provide the information to users when signing up efficiently and succinctly, as well as clearly differentiated from other non-data protection related information.[23] Part of the transparency obligations of the controllers is to inform users about their rights, one of which is to withdraw their consent at any time if consent is the applicable legal basis.[24]

i. Consent provided at the sign-up process stage

25. As Articles 4 (11) and 7 GDPR, clarified by Recital 32, state, when consent is chosen as the legal ground for the processing, it must be "*freely given, specific, informed and [an] unambiguous indication of the data subject's wishes by which he or she, by statement or by a clear affirmative action, signifies*

[21] See Article 2 (1) GDPR.
[22] See Guidelines 04/2019 on Article 25 Data Protection by Design and by Default.
[23] See Guidelines on transparency, para. 8.
[24] Guidelines on transparency, para. 30 and page 39.

agreement to the processing of personal data relating to him or her". All these requirements for consent have to be met cumulatively for it to be considered as valid.

26. For social media providers who ask for users' consent for varying purposes of processing, the EDPB Guidelines 05/2020 on consent provide valuable guidance on consent collection.[25] Social media platforms must not circumvent conditions, such as data subjects' ability to freely give consent, through graphic designs or wording that prevents data subjects from exercising said will. In that regard, Article 7 (2) GDPR states that the request for consent shall be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Users of social media platforms can provide consent for ads or special types of analysis during the sign-up process, and at a later stage via the data protection settings. In any event, as Recital 32 GDPR underlines, consent always needs to be provided by a clear affirmative act, so that pre-ticked boxes or inactivity of the users do not constitute consent.[26]

27. As already highlighted by the EDPB Guidelines on consent, there must be minimum information that users are provided with to meet the threshold of "informed" consent.[27] If this is not the case, the consent acquired during the sign-up process cannot be considered valid under the GDPR, thus rendering the processing unlawful.

28. Users are asked to provide consent to different kinds of purposes (e. g., further processing of personal data). Consent is not specific and therefore not valid when users are not also provided in a clear manner with the information about what they are consenting to.[28] As Article 7 (2) GDPR provides, consent should be requested in a way that clearly distinguishes it from other information, no matter how the information is presented to the data subject. In particular, when consent is requested by electronic means, this consent must not be included in the terms and conditions.[29] Taking into account the fact that a rising number of users access social media platforms using the interface of their smart mobiles to sign up to the platform, social media providers have to pay special attention to the way the consent is requested, to make sure that this consent is distinguishable. Users must not be confronted with excessive information that leads them to skip reading such information. Otherwise, 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. 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".[30] This is also the case where the controller "ties" the provision of a contract or a service to the consent request, so that it processes personal data that are not necessary for the performance of the contract by the controller.

29. While consent must be expressed by a positive action on the part of the users, lack of consent should be considered the default state, until consent has been given. The expression of the users' refusal

[25] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1., adopted on 4 May 2020 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[26] See Court of Justice of the European Union, Judgment from 1 October 2019, *Verbraucherzentrale Bundesverband e.V. v. Planet 49 GmbH*, case C-673/17, para. 62-63.
[27] Guidelines 05/2020 on consent, para. 64; see also below use case 3a in part 3.3. of these Guidelines.
[28] See Guidelines 05/2020 on consent, para. 68.
[29] Guidelines on transparency, para. 8.
[30] See Guidelines 8/2020 on targeting of social media users, para. 57.

should therefore not require any action on their part or should be possible through an action presenting the same degree of simplicity as the one allowing to express their consent.[31]

ii. Withdrawal of consent - Article 7 (3) of the GDPR

30. In accordance with Article 7 (3) phrase 1 GDPR, users of social media platforms shall be able to withdraw their consent at any time. Prior to providing consent, users shall also be made aware of the right to withdraw the consent, as required by Article 7 (3) phrase 3 GDPR. In particular, controllers shall demonstrate that users have the possibility to refuse providing consent or to withdraw the consent without any detriment. Users of social media platforms who consent to the processing of their personal data with one click, for example by ticking a box, shall be able to withdraw their consent in an equally easy way.[32] This underlines that consent should be a reversible decision, so that there remains a degree of control for the data subject related to the respective processing.[33] The easy withdrawal of consent constitutes a prerequisite of valid consent under Article 7 (3) phrase 4 GDPR and should be possible without lowering service levels.[34] As an example, 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,[35] is more difficult to achieve or takes more time.

c. Deceptive design patterns

31. Several GDPR provisions pertain to the sign-up process. Therefore, there are a number of deceptive design patterns which can occur when social media providers do not implement the GDPR as appropriate.

i. Content-based patterns

Overloading - Continuous prompting (Annex I checklist 4.1.1)

32. The ***Continuous prompting*** deceptive design pattern occurs when users are pushed to provide more personal data than necessary for the purposes of processing or to agree with another use of their data, by being repeatedly asked to provide additional data or to consent to a purpose of processing. Such repetitive prompts can happen through one or several devices. Users are likely to end up giving in, as they are wearied from having to refuse the request each time they use the platform.

> **Example 1:**
>
> **Variation A:** In the first step of the sign-up process, users are required to choose between different options for their registration. They can either provide an email address or a phone number. When users choose the email address, the social media provider still tries to convince users to provide the phone number, by declaring that it will be used for account security, without providing alternatives on the data that could be or was already provided by the users. Concretely, several windows pop up throughout the sign-up process with a

[31] See Recital 42, phrase 5, of the GDPR.
[32] See Guidelines on transparency, para. 113 et seq.
[33] Guidelines 05/2020 on consent, para. 10.
[34] Guidelines 05/2020 on consent, para. 114.
[35] See Guidelines 05/2020 on consent, para. 114.

field for the phone number, along with the explanation "*We'll use your [phone] number for account security*". Although users can close the window, they get overloaded and give up by providing their phone number.

Variation B: Another social media provider repeatedly asks users to provide the phone number every time they log into their account, despite the fact that users previously refused to provide it, whether this was during the sign-up process or at the last log-in.

33. The example above illustrates the situation where users are continuously asked to provide specific personal data, such as their phone number. While in variation A of the example, this ***Continuous prompting*** is done several times during the sign-up process, variation B shows that users can also be faced with this deceptive design pattern when they have already registered. To avoid this deceptive design pattern, it is important to be particularly mindful of the principles of data minimisation under Article 5 (1) (c) GDPR and, in cases like the one described in example 1 variation A, also of the principle of purpose limitation under Article 5 (1) (b) GDPR. Therefore, when social media providers state that they will use the phone number "for account security", they shall only process the phone number for said security purposes and must not further process the phone number in a manner that goes beyond this initial purpose.

34. 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 sign-up 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.

35. Social network providers should therefore rely on means for security that are easier for users to re-initiate. For example, the social media provider can send users an authentication number via an additional communication channel, such as a security app, which users previously installed on their mobile phone, but without requiring the users' mobile phone number. User authentication via email addresses is also less intrusive than via phone number because users could simply create a new email address specifically for the sign-up process and utilise that email address mainly in connection with the Social Network. A phone number, however, is not that easily interchangeable, given that it is highly unlikely that users would buy a new SIM card or conclude a new phone contract only for the reason of authentication.

36. One should bear in mind that if the aim of such a request is to prove that users are legitimately in possession of the device used to log into the social network, this goal can be achieved by several means, a phone number being only one of them. Thus, a phone number can only constitute one relevant option on a voluntary basis for users. Finally, users need to decide whether they wish to use this mean as a factor for authentication. In particular, for a one-time-verification, users' phone numbers are not needed because the email address constitutes the regular contact point with users during the registration process.

37. The practice illustrated under example 1 variation A may mislead users and render them to unwillingly provide such information, believing that this is necessary to activate or protect the account. However, in reality users were never provided with the alternative (e.g. use of the email for account activation and security purposes). Under example 1 variation B, users are not informed about a purpose of processing. However, this variation still constitutes a ***Continuous prompting*** deceptive design pattern, as the social media provider disregards the fact that users previously refused to provide the phone

number, and keeps asking for it. When users gain the impression that they can only avoid this repeated request by putting in their data, they are likely to give in.

38. In the following example, users are repeatedly encouraged to give the social media platform access to their contacts:

> **Example 2:** A social media platform uses an information or a question mark icon to incite users to take the "optional" action currently asked for. However, rather than just provide information to users who expect help from these buttons, the platform prompts users to accept importing their contacts from their email account by repeatedly showing a pop-up saying "*Let's do it*".

39. Particularly at the stage of the sign-up process, this ***Continuous Prompting*** can influence users to just accept the platform's request in order to finally complete their registration. The effect of this deceptive design pattern is heightened when combined with motivational language as in this example, adding a sense of urgency.

40. The influencing effects of wording and visuals will be further addressed below, when examining the deceptive design pattern ***Emotional Steering***.[36]

Obstructing – Misleading action (Annex I checklist 4.4.3)

41. Another example of a situation where social media providers ask for users' phone numbers without need concerns the use of the platform's application:

> **Example 3:** When registering to a social media platform via desktop browser, users are invited to also use the platform's mobile application. During what looks like another step in the sign-up process, users are invited to discover the app. When they click on the icon, expecting to be referred to an application store, they are asked instead to provide their number to receive a text message with the link to the app.

42. Explaining to users that they need to provide the phone number to receive a link to download the application constitutes ***Misleading action*** 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. When users have completed the sign-up process, they need to be able to use their log-in data (i.e. usually email address and password) to log in regardless of the device they are using, whether they use a desktop or mobile browser or an application. This is underlined even more by the fact that instead of a smartphone, users could wish to install the application on their tablet, which is not linked to a phone number.

Stirring – Emotional steering (Annex I checklist 4.3.1)

43. With the ***Emotional Steering*** deceptive design pattern, wordings or visual elements (such as style, colours, pictures or others) are used in a way that conveys information to users in either a highly positive outlook, making users feel good, safe or rewarded, or a highly negative one, making users feel anxious, guilty or punished. The manner in which the information is presented to users influences their

[36] See para. 43 et seq. in use case 1, as well as the overview of examples in the Annex checklist.

emotional state in a way that is likely to lead them to act against their data protection interests. Impacts of such practices can be even more effective if based on data collected by the platform. Influencing decisions by providing biased information to individuals can generally be considered as an unfair practice contrary to the principle of fairness of processing set in Article 5 (1) (a) GDPR. It can occur throughout the entire user journey within a social media platform. However, at the sign-up process stage, the steering effect can be especially strong, considering the overload of information that users might have to deal with in addition to the steps needed to complete the registration.

44. In the light of the above, ***Emotional Steering*** at the stage of the registration with a social media platform may have an even higher impact on children, the elderly and other groups (i.e. provide more personal data due to lack of understanding of processing activities), considering their vulnerable nature as data subjects.[37] When social media platform services are addressed to children or other vulnerable data subjects, they should ensure that the language used, including its tone and style, is appropriate so that the vulnerable users, as recipients of the message, easily understand the information provided.[38] Considering the vulnerability of children, the elderly and other data subjects, deceptive design patterns may influence these users to share more information, as "imperative" expressions can make them feel obliged to do so, for example to appear popular among peers or because they believe providing the data is mandatory.

45. When users of social media platforms are prompted to give away their data swiftly, they do not have time to "process" and thus really comprehend the information they are provided with, in order to take a conscious decision. Motivational language used by social media platforms could encourage users to subsequently provide more data than required, when they feel that what is proposed by the social media platform is what most users will do and thus the "correct way" to proceed.

> **Example 4:** The social media platform asks users to share their geolocation by stating: "Hey, a lone wolf, are you? But sharing and connecting with others help make the world a better place! Share your geolocation! Let the places and people around you inspire you!"

46. During the sign-up process, the users' goal is to complete the registration in order to be able to use the social media platform. Deceptive design patterns such as ***Emotional Steering*** have stronger effects in this context. These risk to be stronger in the middle or towards the end of the sign-up process compared to the beginning, as users will most of times complete all the necessary steps "in a rush", or be more susceptible to a sense of urgency. In this context, users are more likely to accept to put in all the data they are requested to provide, without taking the time to question whether they should do so. In this sense, the motivational language used by the social media provider can have an influence on users' instant decision, as can the combination of motivational language with other forms of emphasis, such as exclamation marks, as shown in the example below.

> **Example 5:** Social media provider incentivises users to encourage them to share more personal data than actually required by prompting users to provide a self-description: "*Tell us about your amazing self! We can't wait, so come on right now and let us know!*

47. With this practice, social media platforms receive a more detailed profile of their users. However, depending on the case, providing more personal data, e.g. regarding users' personality, might not be necessary for the use of the service itself and therefore violate the data minimisation principle as per Article 5 (1) (c) GDPR. As illustrated in example 5, such techniques do not cultivate users' free will to

[37] See also above, para. 7.
[38] See Guidelines on transparency, para. 18.

provide their data, since the prescriptive language used can make users feel obliged to provide a self-description because they have already put time into the registration and wish to complete it. When users are in the process of registering to an account, they are less likely to take time to consider the description they give or even if they would like to give one at all. This is particularly the case when the language used delivers a sense of urgency or sounds like an imperative. If users feel this obligation, even when in reality providing the data is not mandatory, this can have an impact on their "free will". It also means that the information provided by the social media platform was unclear.

> **Example 6:** The part of the sign-up process where users are asked to upload their picture contains a "?" button. Clicking on it reveals the following message: "*No need to go to the hairdresser's first. Just pick a photo that says 'this is me'.*"

48. Even if the sentences in example 6 aim to motivate users and to seemingly simplify the process for their sake (i. e. no need for a formal picture to sign up), such practices can impact the final decision made by users who initially decided not to share a picture for their account. Question marks are used for questions, and as an icon, users can expect to find helpful information when clicking on it. When this expectation is not met and users are instead prompted once more to take the action they are hesitant about, consent collected without informing users about the processing of their picture would not be valid, failing to meet the requirements of "informed" and "freely given" consent under Article 7 GDPR in conjunction with Article 4 (11) GDPR. The emotion factor therefore has a strong influence on the legitimacy of consent.

Obstructing – Longer than necessary (Annex I checklist 4.4.2)

49. When users try to activate a control related to data protection, but the user journey is made in a way that requires users to complete more steps, compared to the number of steps necessary for the activation of data invasive options, this constitutes the deceptive design pattern ***Longer than necessary***. This pattern is likely to discourage users from activating the data protective controls. In the sign-up process, this can translate into the display of a pop-in or pop-up window asking users to confirm their decision when they choose a restrictive option (e.g. choosing to make their profiles private). The example below illustrates another case of a sign-up process being ***Longer than necessary.***

> **Example 7:** During the sign-up process, users who click on the "skip" buttons to avoid entering certain kind of data are shown a pop-up window asking "*Are you sure?*" By questioning their decision and therefore making them doubt it, social media provider incites users to review it and disclose these kinds of data, such as their gender, contact list or picture. In contrast, users who choose to directly enter the data do not see any message asking to reconsider their choice.

Here, asking users for confirmation that they do not want to fill in a data field can make them go back on their initial decision and enter the requested data. This is particularly the case for users who are not familiar with the social media platform functions. This ***Longer than necessary*** deceptive design pattern tries to influence users' decisions by holding them up and questioning their initial choice, in addition to unnecessarily prolonging the sign-up process, which constitutes a breach of the fairness principle under Article 5 (1) (a) GDPR. The example shows that the deceptive design pattern can bring users to disclose (more) personal data than they initially chose. It describes an imbalance of treatment of users who disclose personal data right away and those who do not: Only those who refuse to disclose the data are asked to confirm their choice, whereas users who do disclose the data are not asked to confirm their choice. This constitutes a breach of the fairness

principle under Article 5 (1) (a) GDPR with regard to users who do not wish to disclose these personal data.

ii. Interface-based patterns

Stirring – Hidden in Plain Sight (Annex I checklist 4.3.2)

50. Pursuant to the principle of transparency, data subjects have to be provided with information in a clear way to enable them to understand how their personal data are processed and how they can control them. In addition, this information has to be easily noticeable by the data subjects. However, information related to data protection, in particular links, are often displayed in such a way that users will easily overlook it. Such practices of ***Hidden in plain sight*** use a visual style for information or data protection controls that nudge users away from data protection advantageous options to less restrictive and thus more invasive options.

51. Using small font size or a colour which does not contrast sufficiently to offer enough readability (e. g., faint grey text colour on a white background) can have negative impact on users, as the text will be less visible and users will either overlook it or have difficulties reading it. This is especially the case when one or more eye-catching elements are placed next to the mandatory data protection related information. These interface techniques mislead users and render the identification of information related to their data protection more burdensome and time-consuming, as it requires more time and thoroughness to spot the relevant information.

> **Example 8:** Immediately after completing the registration, users are only able to access data protection information by calling up the general menu of the social media platform and browse the submenu section that includes a link to "*privacy and data settings*". Upon a visit to this page, a link to the privacy policy is not visible at first glance. Users have to notice, in a corner of the page, a tiny icon pointing to the privacy policy, which means that users can hardly notice where the information to the data protection related policies are.

52. It is important to note that even when social media providers make available all the information to be provided to data subjects under Article 13 and 14 GDPR, the way this information is presented can still infringe the overarching requirements of transparency under Article 12 (1) GDPR. When the information is ***Hidden in plain sight*** and therefore likely to be overlooked, this leads to confusion or disorientation and cannot be considered intelligible and easily accessible, contrary to Article 12 (1) GDPR.

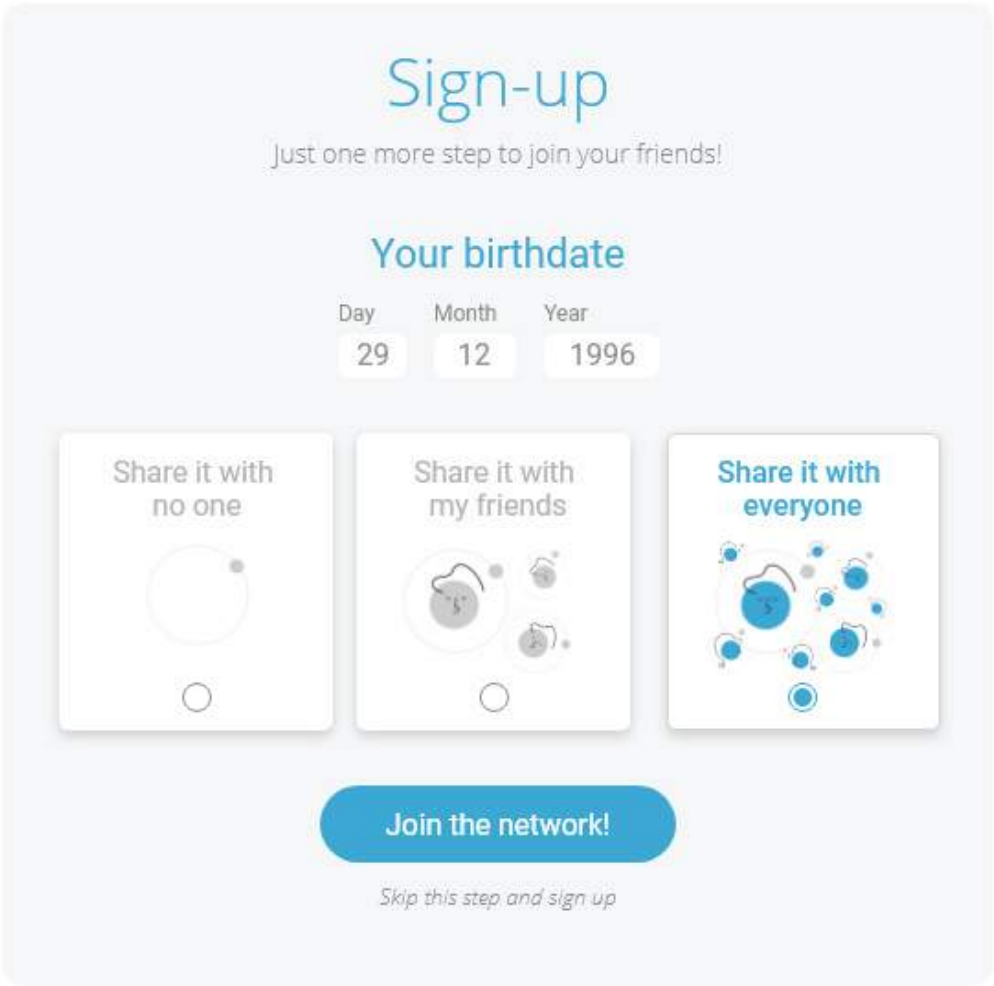
53. While the example above shows the deceptive design pattern after completion of the sign-up process, this pattern also already occurs during the sign-up process, as will be shown in the example illustrated below, which combines the ***Hidden in plain sight*** and ***Deceptive snugness*** patterns.

Skipping – Deceptive snugness (Annex I checklist 4.2.1)

54. Social media providers also need to be mindful of the principle of data protection by default. When data settings are pre-selected, users are subject to a specific data protection level, determined by the provider by default, rather than by users. In addition, users are not always immediately provided with the option to change the settings to stricter, data protection compliant ones. Compliance with the GDPR in this regard does not mean that all options need to look exactly the same. However, if social

media providers highlight one of the options and thus raise the users' attention to it, this needs to be the most restrictive one regarding personal data, in order to comply with, inter alia, the principle of data minimisation under Article 5 (1) (c) GDPR.

55. When the most data invasive features and options are enabled by default, this constitutes the pattern ***Deceptive Snugness***. Because of the default effect which nudges individuals to keep a pre-selected option, users are unlikely to change these even if given the possibility. This practice is commonly met in sign-up processes, as illustrated in example 9 below, since it is an effective way to activate data invasive options that users would otherwise likely refuse. Such deceptive design patterns conflict with the principle of data protection by default of Article 25 (2) GDPR, especially when they affect the collection of personal data, the extent of the processing, the period of data storage and data accessibility.[39]



Example 9: In this example, when users enter their birthdate, they are invited to choose with whom to share this information. Whereas less invasive options are available, the option *"share it with everyone"* is selected by default, meaning that everyone, i.e. registered users as well as any internet users, will be able to see the users' birthdate.

[39] See also para. 446 of the Final Decision of the Irish Data Protection Authority regarding Instagram (Meta Platforms Ireland Limited) following the EDPB's binding dispute resolution decision of 28 July 2022, https://edpb.europa.eu/news/news/2022/record-fine-instagram-following-edpb-intervention_en.

56. Example 9 shows 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. In addition, the default effect of this pattern nudges users to keep the pre-selection, i. e. to neither take time to consider the other options at this stage nor to go back to change the setting at a later stage. The ***Hidden in Plain Sight*** pattern is also used in this interface. Indeed, entering one's birthdate is not mandatory as users can skip this sign-up step by clicking on the link saying *"Skip this step and sign up"* that is available below the *"Join the network!"* button. The fact that the birthdate field and the confirmation button are so prominent is likely to nudge users into entering their birthdate and sending it to the social network because they do not notice the possibility of not sharing this information. This effect would be even stronger if animated circles were used next to the field and button which strongly attract users' attention.

57. Respecting the principle of data protection by design and default does not mean that all options on offer need to look exactly the same. However, if controllers decide to highlight one option more than the other(s), the highlighted one needs to be the most restrictive regarding data processing.

58. Besides nudging users into keeping an option that does not necessarily match their preferences, social media providers might not prompt users to verify or modify their data protection settings according to their preferences after completing the sign-up process. Moreover, changing these default settings could require several steps. When users are not in any way prompted to verify or modify their data protection settings or are not directed in a clear manner to any related information, their data protection level will depend on their own initiative. To facilitate users' control of their data, so-called privacy dashboards can be used that are designed to centralise and ease such endeavour.

59. It is important to keep in mind that the lack of data protection by design and default, in combination with the above-mentioned default effect can have harmful consequences for data subjects, including to their cyber security. Publicly displaying personal data, such as the birthdate, which is used for verification processes by other online services could make it easier for criminals to gain access to users' shopping, banking and other accounts. Another harmful consequence concerns contact possibilities on the social media platform: if the default option for sending contact requests or messages to users is set to "anyone", this raises the risk for cyber-grooming and fraud, especially on vulnerable groups.

60. Finally, when ***Deceptive Snugness*** is applied to the collection of consent, which would equate with considering that users consent by default, for example by using a pre-ticked box or considering inactivity as approval, conditions for consent set in Article 4 (11) GDPR are not met and the processing would be considered unlawful under Articles 5 (1) (a) and 6 (1) (a) GDPR.

Obstructing – Dead end (Annex I checklist 4.4.1)

61. It is important to point out that the sign-up process stage is a defining moment for users to get informed. If they are looking for information and cannot find it as no redirection link is available or working, this constitutes a ***Dead end*** pattern because users are left unable to achieve that goal.

> **Example 10:** Users are not provided with any links to data protection information once they have started the sign-up process. Users cannot find this information as none is provided anywhere in the sign-up interface, not even in the footer.

62. In practice, this example entails that users will only be able to either stop the registration and go back to the start page if this contains a link to the privacy notice, or to complete the registration, log in to

the social media platform and only then have access to data protection related information. This infringes the principle of transparency and easy access to information that data subjects shall be provided with as required in Article 12 (1) GDPR. It also fails to meet the requirements of Article 13 (1) and (2) GDPR as no information is provided and accessible at the time when personal data are obtained.

63. The ***Dead end*** pattern can also occur in another way when users are provided with a data protection related action or option during the sign-up process that they cannot find again later, while using the service.

> **Example 11:** During the sign-up process, users can consent to the processing of their personal data for advertising purposes and they are informed that they can change their choice whenever they want once registered on the social media by going to the privacy policy. However, once users have completed the registration process and they go to the privacy policy, they find no means or clues on how to withdraw their consent for this processing.

64. In this specific example, users have no mean to withdraw their consent once signed up. Here, the deceptive design pattern ***Dead end*** infringes the data subjects' right to withdraw consent at any time, and as easily as giving consent, under Article 7 (3) phrases 1 and 4 GDPR.

65. Finally, pointing users to a link that supposedly leads them to data protection related pages, such as settings or data protection information, is also an example of a ***Dead end*** pattern if the link is broken and no fall-back links are made available that would help users find what they are looking for. This way, users cannot seek for the relevant information, while no explanations are provided to them, such as the reason why this takes place (e.g. technical issues). In such a case, the same issues related to transparency and easy access to information as described in para. 58 occur.

d. Best practices

To design user interfaces which facilitate the effective implementation of the GDPR, the EDPB recommends implementing the following best practices for the sign-up process:

Shortcuts: Links to information, actions or settings that can be of practical help to users to manage their data and their data protection settings should be available wherever they are confronted to related information or experience (*e.g. links redirecting to the relevant parts of the privacy policy*).

Contact information: The company contact address for addressing data protection requests should be clearly stated in the privacy policy. It should be present in a section where users can expect to find it, such as a section on the identity of the data controller, a rights related section or a contact section.

Reaching the supervisory authority: Stating the specific identity of the supervisory authority and including a link to its website or the specific website page related to lodging a complaint. This information should be present in a section where users can expect to find it, such as a rights related section.

Privacy Policy Overview: At the start / top of the privacy policy, include a (collapsible) table of contents with headings and sub-headings that shows the different passages the privacy notice contains. The names of the single passages clearly lead users regarding the exact content and allow them to quickly identify and jump to the section they are looking for.

Change spotting and comparison: When changes are made to the privacy notice, make previous versions accessible with date of release and highlight changes.

Coherent wordings: Across the website, the same wording and definition is used for the same data protection. The wording used in the privacy policy should match the one used on the rest of the platform.

Providing definitions: When using unfamiliar or technical words or jargon, providing a definition in plain language will help users understand the information provided to them. The definition can be given directly into the text, when users hover over the word, as well as be made available in a glossary.

Contrasting Data protection elements: Making data protection related elements or actions visually striking in an interface that is not directly dedicated to the matter. For example, when posting a public message on the platform, controls over association of the geolocation should be directly available and clearly visible.

Data Protection Onboarding: Just after the creation of an account, include data protection points within the onboarding experience of the social media provider for users to smoothly discover and set their preferences. For example, this can be done by inviting them to set their data protection preferences after adding their first friend or sharing their first post.

Use of examples: In addition to mandatory information clearly and precisely stating the purpose of processing, examples can be used to illustrate a specific data processing to make it more tangible for users.

Contextual information: in addition to an exhaustive privacy policy, bring short bits of information at the most appropriate time for the user to have a specific and continuous information on how their data are processed.

3.2 Staying informed on social media

Use case 2a: A layered privacy notice

a. **Description of the context**

66. As already highlighted in the Guidelines on transparency, the principle of transparency is very closely linked to the principle of fair processing of personal data.[40] However, information about the processing of personal data also makes data controllers reflect on their own actions, makes data processing more comprehensible for data subjects, and ultimately empowers data subjects to have control over their data, especially by exercising their rights. The resulting equalisation of abilities of the persons involved leads to a fair system of processing personal data. However, more information does not necessarily mean better information. Too much irrelevant or confusing information can obscure important content points or reduce the likelihood of finding them. Hence, the right balance between content and comprehensible presentation is crucial in this area. If this balance is not met, deceptive design patterns can occur.

b. **Relevant legal provisions**

67. The relationships just outlined become clear on the basis of Article 5 GDPR. Transparency and fairness are already systematically mentioned side by side in Article 5 (1) (a) GDPR, as one component determines the other. The fact that not only external but also internal transparency must exist is also made clear by the accountability requirement in Article 5 (2) GDPR. The most important part of internal transparency is the requirement to keep a record of processing activities under Article 30 GDPR. For

[40] Guidelines on transparency, p. 4-5.

external transparency, social media providers can provide a layered privacy notice to users, among other means of information.[41] This need for comprehensibility and fair processing also results in the requirements of Article 12 (1) GDPR, which state that any information referred to in Articles 13 and 14 GDPR shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Consequently, the information content must be made available without obstacles. If the requirements of Article 12 GDPR are not met, there is no valid information within the meaning of Articles 13 and 14 GDPR. Thus, for effective control, controllers and processors can be held accountable, leading to effectiveness of the GDPR requirements in practice.

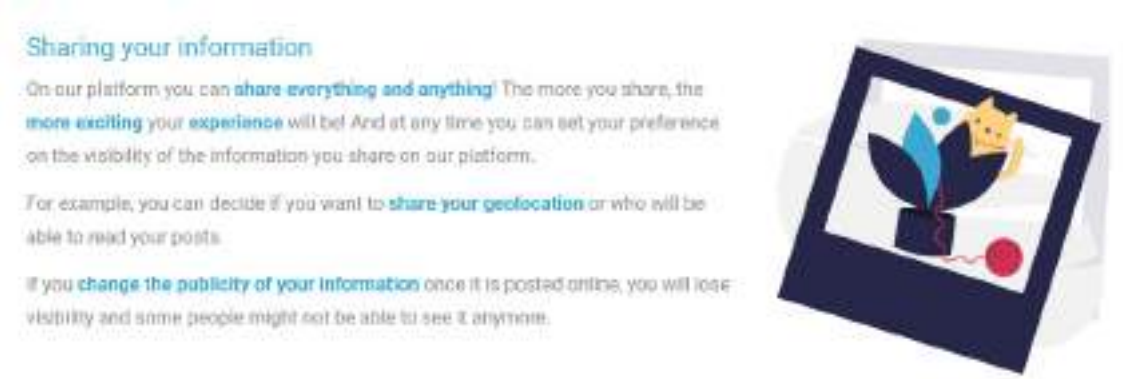
c. Deceptive design patterns

i. Content-based patterns

68. Regarding this use case, content-based patterns find their limits in Article 12 (1) GDPR, which requires a precise and intelligible form as well as clear and plain language regarding the information provided.

Left in the Dark – Conflicting Information (Annex I checklist 4.6.2)

69. One of the most obvious cases where this can occur is when ***Conflicting Information*** is given, which leaves users unsure of what they should do and of the consequences of their actions, therefore not taking any, or keeping the default settings.



Example 12: In this example, the information related to data sharing gives a highly positive outlook of the processing by highlighting the benefits of sharing as many data as possible. Coupled to the illustration representing the photograph of a cute animal playing with a ball, this ***Emotional Steering*** can give users the illusion of safety and comfort with regard to the potential risks of sharing some kind of information on the platform. On the other hand, information given on how to control the publicity of one's data is not clear. First it is said that users can set their sharing preference any time they want. Then, however, the last sentence indicates that this is not possible once something has already been posted on the platform. Those pieces of ***Conflicting Information*** leave users unsure of how to control the publicity of their data.

[41] See Use case 2.a in Section 3.2 below.

Fickle – Lacking Hierarchy (Annex I checklist 4.5.1)

71. Similar effects as with ***Conflicting Information*** and ***Emotional Steering*** can occur if the presentation of the information does not follow an internal system or any hierarchy. Information related to data protection which is ***Lacking Hierarchy*** occurs when said information appears several times and is presented in several different ways. Users are likely to be confused by this redundancy and to be left unable to fully understand how their data are processed and how to exercise control over them. Such architecture makes information hard to understand, as the complete picture is not easily accessible. In cases as the one described in the following example, this infringes the requirements of intelligibility and ease of access under Article 12 (1) GDPR.

> **Example 13:** Information related to data subject rights is spread across the privacy notice. Although different data subject rights are explained in the section "*Your options*", the right to lodge a complaint and the exact contact address is stated only after several sections and layers referring to different topics. The privacy notice therefore partly leaves out contact details at stages where this would be desirable and advisable.

72. ***Lacking Hierarchy*** can also emerge when the given information is structured in a way that makes it hard for users to orientate, as the following example shows.

> **Example 14:** The privacy policy is not divided into different sections with headlines and content. There are more than 70 pages provided. However, there is no navigation menu on the side or the top to allow users to easily access the section they are looking for. The explanation of the self-created term *"creation data"* is contained in a footnote on page 67.

Left in the Dark – Ambiguous Wording or Information (Annex I checklist 4.6.3)

73. Even if the choice of words is not overtly contradictory, problems can arise from the use of ambiguous and vague terms when giving information to users. With such information, users are likely to be left unsure of how data will be processed or how to have some control over the data. If it can be assumed that average users would not understand the genuine message of the information without special knowledge, the conditions of Article 12 (1) GDPR are not met. By extension, the use of ***Ambiguous wording or information*** can contradict the principle of fairness of Article 5 (1) (a) GDPR, since information cannot be considered transparent, making data subjects unable to understand the processing of their personal data and to exercise their rights.

> **Example 15:** 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*". Additionally, the right of access to personal data is applicable to the processing as based on Article 15 (1) GDPR but is mentioned in such a way that it is not clear to users what it allows them to access: "*You can see part of your information in your account and by reviewing what you've posted on the platform".*

74. In the example, the use of conditional tense ("*might*") leaves users unsure whether their data will be used for the processing or not. The term *"services"* is likely to be too general to qualify as "clear". In addition, it is unclear how data will be processed for the improvement of services. The EDPB recalls that the use of conditional tense or vague wording does not constitute "clear and plain language" as

required by Article 12 (1) phrase 1 GDPR and may only be used if controllers are able to demonstrate that this does not undermine the fairness of processing.[42]

Fickle – Language discontinuity (Annex I checklist 4.5.4)

75. When online services are offered and addressed to residents of certain Member States, the data protection notices should also be offered in these languages.[43] In this context, it is important that the choice of a particular language can also be switched manually and is implemented continuously without interruptions. If these criteria are not met, data subjects are confronted with a ***Language Discontinuity***, leaving them unable to understand information related to data protection. Users will face this deceptive design pattern when data protection information is not provided in the official languages of the country where they live, whereas the service is provided in that language. If users do not master the language in which data protection information is given, they will not be able to read it easily and therefore will not be aware of how their personal data are processed. It is important to note that ***Language Discontinuity*** can confuse users and create a settings environment that they do not understand how to make use of. This deceptive design pattern can appear in various ways, as will be shown throughout these Guidelines.

Example 16:

Variation A: The social media platform is available in Croatian as the language of users' choice (or in Spanish as the language of the country they are in), whereas all or certain information on data protection is available only in English.

Variation B: Each time users call up certain pages, such as the help page, these automatically switch to the language of the country users are in, even if they have previously selected a different language.

76. Variation A illustrates the case where no information is available in a language apparently mastered by the data subject. This means that they cannot read the information and by extension cannot understand how their personal data are processed. Information cannot be considered intelligible as required in Article 12 (1) GDPR. Due to the lack of data protection information in the understandable language, the information required under Article 13 respectively 14 GDPR cannot be considered to have been given to data subjects.

77. Variation B describes a case where data protection information pages are by default presented in the language of the users' country of residence despite their clear language choice. This means that users have to reset their language preference each time they access a data protection information page. This can be considered as an unfair practice towards data subjects and could contribute to a breach of the principle of fairness of Article 5 (1) (a) GDPR.

ii. Interface-based patterns

78. In some cases, social media providers make use of specific practices to present their data protection settings. During the sign-up process, users are provided with a lot of information and different settings related to data protection. To make sure users can find their way to these settings and make changes

[42] See Guidelines on transparency, para. 12, including the "Poor Practice Examples", and para. 13.
[43] See Guidelines on transparency, para. 13 and footnote 15.

at any point when using the platform, the settings should be easily accessible and associated with relevant information for users to make an informed decision. The "easily accessible" element means that data subjects should not have to seek out the information. Regarding privacy policies, the Article 29 Working Party has already stated that a positioning or colour schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible.[44]

Overloading – Privacy Maze (Annex I checklist 4.1.2)

79. According to the Guidelines on Transparency, the privacy notice should be easily accessible, i.e. through one click on websites.[45] Using the method of layered approach can help present the privacy notice more clearly in the sense of Article 12 (1) GDPR.[46] However, this should not result in making the exercise of important functions or rights unnecessarily difficult by providing a complex privacy policy consisting of innumerable layers that would result in the deceptive design pattern ***Privacy Maze***. This pattern corresponds to an information or data protection control being particularly difficult to find, as users have to navigate through many pages without having a comprehensive and exhaustive overview available. This is likely to make users overlook the relevant information/setting or to give up looking for them. The layered arrangement is intended to facilitate readability and give information on how to exercise data subject rights, not to make them more difficult. It is central to ensure that users can easily follow the explanations.

80. In that regard, what is best for users is not a one-size-fit-all approach and depends on many criteria, such as the kind of users on the platform or the general type of design of the application. Where possible, testing the implemented layered approach with users to get their feedback should be carried out to assess its effectiveness. For this reason, no concrete number can be quantified for the maximum number of information layers permissible. It must therefore always be determined on a case-by-case basis whether too many layers are used and thus deceptive design patterns occur. However, the higher the number, the more it can be assumed that users will be discouraged or misled. A high number of layers will only be appropriate for special individual cases in which it is not easy to provide the complex information comprehensively. At the same time, the layered approach may not be misused to hide information in deeper layers or by adding unnecessary layers.

81. However, this is to be assessed differently when it comes to the exercise of the rights of the users. The GDPR requires that the exercise of these rights is always granted. This framework determines the presentation of information on related functions and the exercise of rights. When users want to exercise their rights, the number of steps should be as low as possible. As a result, users should get to the function that allows them to exercise their rights as directly as possible. In most cases, having to navigate a high number of information layers before users can actually exercise their rights through functions could discourage them from exercising these rights. If a high number of steps are implemented, the social media provider should be able to demonstrate the benefit this has for users as data subjects under the GDPR. In addition to the explanation of data subject rights in the privacy notice, as required by Article 13 (2) (b), (c) and (d) GDPR, the exercise of rights should also be accessible independently from this information. For example, users should be able to exercise data subject rights via the platform's menu as well.

[44] Guidelines on transparency, para. 11.
[45] See Guidelines on transparency, example in para. 11.
[46] For details on the layered approach in a digital environment, see Guidelines on transparency, para. 35-37.

> **Example 17:** On its platform, the social media provider makes available a document called "*helpful advice*" that also contains important information about the exercise of data subject rights. However, the privacy policy does not contain any link or other hint to this document. Instead, it mentions that more details are available in the Q&A section of the website. Users expecting information about their rights in the privacy policy will therefore not find these explanations there and will have to navigate further and search through the Q&A section.

82. This example clearly shows a ***Privacy Maze*** pattern that makes access to further information to the data subject rights, and in particular on how to exercise them, harder to find than it should, contrary to Article 12 (2) GDPR. In addition, if the privacy policy is incomplete, this also infringes Article 13 (2) (b), (c) and (d), respectively Article 14 (2) (c), (d) and (e) GDPR. Indeed, whereas more detailed information or the direct mean to exercise the rights could be one click away from where they are mentioned in the privacy policy, users in the example will have to navigate to the Q&A and search it in order to find the "*helpful advice"* document.

83. It is important to note that even stronger effects than those caused by too many layers[47] can occur when not only several devices, but also several apps provided by the same social media platform, such as special messenger apps, are used. Users who use that kind of secondary app would face greater obstacles and efforts if they have to call up the browser version or the primary app to obtain data protection related information. In such a situation, which is not only cross-device but cross-application, the relevant information must always be directly accessible no matter how users use the platform.

Obstructing – Dead end (Annex I checklist 4.4.1)

84. Violations of legal requirements can also occur when data protection information required by the GDPR is made available through further actions, such as clicking on a link or a button. In particular, misdirected navigation or inconsistent interface design that leads to ineffective features cannot be classified as fair under Article 5 (1) (a) GDPR, as users are misled when they either try to reach some information or set their data protection preferences. ***Dead ends*** where users are left alone without functions to pursue their rights should therefore be avoided in any case and directly violate Article 12 (2) GDPR stating that the controller has to facilitate the exercise of rights.

> **Example 18:** In its privacy policy, a social media provider offers many hyperlinks to pages with further information on specific topics. However, there are several parts in the privacy policy containing only general statements that it is possible to access more information, without saying where or how.

85. The privacy policy is generally viewed as the document that centralises all information concerning data protection matters in accordance with the obligations set in Articles 12, 13 and 14 GDPR. Therefore, it is necessary to also ensure redirection to all the relevant places on the social media platform for users to control their data or exercise their rights. In example 18 above, this is only partly implemented, as links to further information are provided for some elements, but not for others. For these, the ***Dead end*** pattern can lead to a breach of Article 12 (1) GDPR, by making some data protection information hard to access, or of Article 12 (2) GDPR, by not facilitating the exercise of the rights.

d. **Best practices**

[47] See above, para. 81 and 82.

Sticky navigation: While consulting a page related to data protection, the table of contents can be constantly displayed on the screen allowing users to always situate themselves on the page and to quickly navigate in the content thanks to anchor links.

Back to top: Include a return to top button at the bottom of the page or as a sticky element at the bottom of the window to facilitate users' navigation on a page.

Shortcuts: see use case 1 for definition (p. 22). (*e.g. in the privacy policy, provide for each data protection information links that directly redirects to the related data protection pages on the social media platform*).

Contact information: see use case 1 for definition (p. 22).

Reaching the supervisory authority: see use case 1 for definition (p. 22).

Privacy Policy Overview: see use case 1 for definition (p.22).

Change spotting and comparison: see use case 1 for definition (p. 22).

Coherent wordings: see use case 1 for definition (p. 22).

Providing definitions: see use case 1 for definition (p. 22).

Use of examples: see use case 1 for definition (p. 22).

Use case 2b: Providing information about joint controllership to the data subject, Article 26 (2) GDPR

a. Description of the context and relevant legal provisions

86. The second phrase of Article 26 (2) GDPR provides for additional transparency provisions in the specific case of joint controllership.[48] These ensure that the essence of the joint controllership agreement is made available to the data subjects.[49] In its Guidelines 07/2020 on the concepts of controller and processor in the GDPR, the EDPB recommends that the essence cover at least all the elements of the information referred to in Articles 13 and 14 GDPR that should already be accessible to data subjects, and to specify for each element which joint controller is responsible for ensuring compliance with it.[50] The essence of the arrangement must also indicate the contact point, if designated. It is up to the joint controllers to decide the most effective way to make the essence of the arrangement available to the data subjects.[51]

b. Deceptive design patterns

Example 19: With regard to deceptive design patterns, the challenge for controllers in this constellation is to integrate this information into the online system in such a way that it can be easily perceived and does not lose its clarity and comprehensibility, even though Article 12 (1) phrase 1 GDPR does not refer directly to Article 26 (2) phrase 2 GDPR.

[48] For the definition of joint controllership, see Article 4 (7) in conjunction with Article 26 (1) phrase 1 GDPR, as well as the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, adopted on 7 July 2021, version 2.1, para. 46-49, available at https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf.
[49] See EDPB Guidelines 07/2020 on controller and processor, para. 179.
[50] See EDPB Guidelines 07/2020 on controller and processor, para. 180, also for next sentence.
[51] EDPB Guidelines 07/2020 on controller and processor, para. 181.

However, due to the data protection principles of fairness, transparency and accountability under Article 5 (1) (a) and (2) GDPR, comparable requirements derive as well to the case of joint controllership. When joint controllers provide information about the essence of the arrangement in a privacy notice, this also needs to be done in a clear and transparent way. Therefore, the processing can no longer be assessed as fair if the information about it is made difficult to grasp because links are not provided or the information is spread across several information areas. The deceptive design pattern ***Privacy Maze***[52] could be even more confusing than, generally, in a privacy notice, as users can expect the information according to Article 26 (2) phrase 2 GDPR to be given in one piece. A Social Media Provider always refers to *"creation data"* within the privacy policy and does not use the term personal data. Only on page 90, the layered privacy notice contains the explanation that *"creation data might include personal data of the users"*. The essence of the joint controller agreement provided to data subjects also uses the term "creation data", without explanation. The other joint controller (B) has a definition of personal data in its own privacy policy. However, in its privacy policy section about joint controllership with the social media provider, B only provides a link to the agreement provided by the social media provider, without other explanation.

87. The explanations under Article 26 (2) phrase 2 GDPR are more difficult to conceive when they are no longer coherent. This incoherence effect is amplified when social media platforms use self-created terminology which users do not usually associate with the processing of personal data, as shown in example 19 above. In the example, both of the joint controllers infringe Article 26 (2) phrase (2) GDPR, as well as Article 5 (1) (a) GDPR because the information provided on joint controllership is unclear and therefore not transparent for data subjects.

Use case 2c: Communication of a personal data breach to the data subject

a. Description of the context and relevant legal provisions

88. To be able to identify and address a data breach, a controller has to be able to recognize one.[53] According to Article 4 (12) GDPR, "personal data breach" means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". When it comes to social media controllers, data breaches can happen in several ways. For example, if an attacker manages to access personal data and users' chat messages. Alternatively, due to a programming failure, an app could access personal data outside the scope of the permissions granted by users. Another example would be that users share pictures under the setting "share with my best friends", but their pictures are made available to a wider range of people instead. As a last example, a bug could allow a social media platform based on real-time video to share further streaming of content despite the fact that users had previously pressed a button to stop the recording.

89. If a personal data breach occurs, a controller shall, in any event, notify the competent supervisory authority according to Article 33 GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If a data breach is likely to result in a high risk to the rights

[52] See above, use case 2a, example 17 in these Guidelines.
[53] See also EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification, adopted on 14 December 2021, Version 2.0, para. 4, available at https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf.

and freedoms of natural persons, the controller shall, in general, also communicate such a breach to the data subjects according to Article 34 (1) and (2) GDPR. In this case, the controller must inform the data subjects without undue delay. This information must describe in clear and plain language the nature of the personal data breach, as Article 12 GDPR also applies. Moreover, this information must contain at least information and measures such as (see also Article 33 (3) (b) to (d) in conjunction with Article 34 (2) GDPR):

- the name and contact details of the data protection officer (DPO), if applicable, or another contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate measures to mitigate its possible adverse effects.[54]

90. Such data breach communications under Article 34 GDPR can also contain deceptive design patterns. For example, if the respective controller provides all the necessary information to the data subjects to inform them about the scope of the data breach but also provides them with unspecific and irrelevant information and the implications and precautionary measures the controller has taken or suggests to take. This partly irrelevant information can be misleading and users affected by the breach might not fully understand the implications of the breach or underestimate the (potential) effects.

b. Deceptive design patterns

91. To outline some negative examples, malpractices of data breach notifications, infringing Article 34 GDPR in conjunction with Article 12 GDPR, could occur as follows:

i. Content-based patterns

Left in the Dark – Conflicting Information (Annex I checklist 4.6.2)

Example 20:

- The controller only refers to actions of a third party, that the data breach was originated by a third party (e.g. a processor) and that therefore no security breach occurred. The controller also highlights some good practices that have nothing to do with the actual breach.
- The controller declares the severity of the data breach in relation to itself or to a processor, rather than in relation to the data subject.

Left in the dark – Ambiguous wording or information (Annex I checklist 4.6.3)

92. When it comes to the language of the communication of the breach to the data subject, it is crucial for controllers to keep in mind that most recipients will not be used to specific, maybe technical or legal data protection related language.

[54] Article 29 Working Party Guidelines on personal data breach notification, endorsed by the EDPB, p. 20 https://ec.europa.eu/newsroom/article29/items/612052/en.

> **Example 21:** Through a data breach on a social media platform, several sets of health data were accidentally accessible to unauthorised users. The social media provider only informs users that "*special categories of personal data*" were accidentally made public.

93. This constitutes ***Ambiguous wording***, as average users do not understand the term "*special categories of personal data"* and therefore do not know that their health data has been leaked. This is due to the fact that "special" has a very different meaning in general language than "special" in the narrow GDPR-related language use. Average users do not know that under Article 9 (1) GDPR, *"special categories of personal data"* relate to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or genetic data, biometric data for the purpose of uniquely identifying a natural person, or to data concerning health or data concerning a natural person's sex life or sexual orientation. Thus, the designation *"special categories of personal data"* constitutes a deceptive design pattern in this scenario, as it misleads users because it is not accompanied with further explanations. This is an example of a situation in which a controller tries to inform data subjects about the breach, but fails to fully comply with its obligation to communicate the data breach in accordance with Article 34 GDPR because the seriousness of the incident will be underestimated by the average reader. The short information in the example is also not intelligible, as required by Article 34 in conjunction with Article 12 (1) phrase 1 GDPR.

94. Another example of ***Ambiguous wording*** is the following:

> **Example 22:** The controller only provides vague details when identifying the categories of personal data affected, e. g. the controller refers to documents submitted by users without specifying what categories of personal data these documents include and how sensitive they were.

95. It is important to note that this deceptive design pattern can occur in all parts of the data breach notification. Whereas the two above-mentioned examples refer to unclear wording about the affected data categories, the next example shows that the category of affected data subjects could be equally unclear:

> **Example 23:** When reporting the breach, the controller does not sufficiently specify the category of the affected data subjects, e. g., the controller only mentions that concerned data subjects were students, but the controller does not specify whether the data subjects are minors or groups of vulnerable data subjects.

96. Finally, the seriousness of the incident can also be underestimated when ***Ambiguous information*** is given similarly to the example below:

> **Example 24:** A controller declares that personal data was made public through other sources when it notifies the breach to the Supervisory Authority and to the data subject. Therefore, the data subject considers that there was no security breach.

ii. Interface-based patterns

97. Negative examples of a data breach notification, contrary to Article 34 GDPR in conjunction with Article 12 GDPR, can also constitute interface-based deceptive design patterns, as shown in the following:

Skipping – Look over there (Annex I checklist 4.2.2)

Example 25:

- The controller reports through texts that contain a lot of non-relevant information and omit the relevant details.
- In security breaches that affect access credentials and other types of data, the controller declares that the data is encrypted or hashed, while this is only the case for passwords.

98. In this case, even if the relevant details are in the report, data subjects are likely to be deflected from it by an overload of irrelevant information.

c. Best practices

Notifications: Notifications can be used to raise awareness of users on aspects, change or risks related to personal data processing (*e.g. when a data breach occurred*). These notifications can be implemented in several ways, such as through inbox messages, pop-in windows, fixed banners at the top of the webpage, etc.

Explaining consequences: When users want to activate or deactivate a data protection control, or give or withdraw their consent, inform them in a neutral way on the consequences of such action.

Shortcuts: see use case 1 for definition (p.22) (*e.g. provide users with a link to reset their password*).

Coherent wordings: see use case 1 for definition (p.22).

Providing definitions: see use case 1 for definition (p.22).

Use of examples: see use case 1 for definition (p.22).

3.3 Staying protected on social media

Use case 3a: Managing one's consent while using a social media platform

a. Description of the context and relevant legal provisions

99. Social media platform users need to provide their respective consent during different parts of data processing activities, for example before receiving personalized advertisement. As already outlined in the EDPB Guidelines on Targeting of Social Media Users, consent can only be an appropriate legal basis if a data subject is offered control and genuine choice.55 In addition, according to Article 4 (11) GDPR, consent must be specific, informed and unambiguous.56 It is important to underline that the requirements for valid consent under the GDPR do not constitute an additional obligation, but are preconditions for lawful processing of users' personal data. Moreover, when online marketing or online tracking methods are concerned, Directive 2002/58/EC (e-Privacy Directive) is applicable. However, the prerequisites for valid consent under the e-Privacy Directive are identical to the provisions related to consent in GDPR.57

[55] Guidelines 08/2020 on the targeting of social media users, para 51.
[56] See also para. 25-29 above.
[57] See Article 2(f) of Directive 2002/58/EC as well as EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019, para 14, https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_en.

100. Given the principle of accountability laid down in Article 5 (2) GDPR, as well as the necessity for the controller to be able to demonstrate that data subjects have consented to the processing of their personal data under Article 7 (1) GDPR, it is crucial that the social media provider can prove having properly collected users' consent. This condition can become a challenge to prove, e.g. if users are supposed to provide consent by accepting cookies. Furthermore, data subjects might not always be aware that they are giving consent while they click quickly on a highlighted button or on pre-set options. Nevertheless, as Article 7 (1) GDPR underlines, the burden of proof that users have freely given consent relies on the controller.

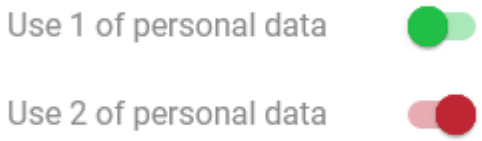
b. Deceptive design patterns

i. Content-based patterns

101. In addition to the content-based patterns already explained previously that could apply to the information related to a consent request,[58] two more content-based deceptive design patterns can be found in relation to consent.

Conflicting Information – Left in the Dark (Annex I checklist 4.6.2)

Example 26: The interface uses a toggle switch to allow users to give or withdraw consent. However, the way the toggle is designed does not make it clear in which position it is and if users have given consent or not. Indeed, the position of the toggle does not match the colour. If the toggle is on the right side, which is usually associated with the activation of the feature ("switch on"), the colour of the switch is red, which usually signifies that a feature is turned off. Conversely, when the switch is on the left side, usually meaning the feature is turned off, the toggle background colour is green, which is normally associated with an active option.



102. Giving ***Conflicting Information*** when collecting consent makes the information unclear and unintelligible. The example above illustrates a case where the visual information is equivocal. Indeed, confronted to such toggles, users will be unsure if they gave their consent or not. When visual signifiers are mixed up in such a way or presented in other colours that appear contradictory to the actual setting – example 26 containing only one illustration of confusing toggles –, consent cannot be considered as given in an unambiguous way, under Article 7 (2) GDPR, in conjunction with Article 4 (11) GDPR. ***Conflicting Information*** can also be given by textual means as shown below.

[58] See use case 1, para. 32-49, or UC1 example numbers listed in the Annex.

Example 27: The social media provider gives contradictory information to users: Although the information first asserts that contacts are not imported without consent, a pop-up information window simultaneously explains how contacts will be imported anyway.

Obstructing – Misleading action (Annex I checklist 4.4.3)

103. Besides providing ***Conflicting Information***, controllers can implement information that misleads users by not matching their expectations. ***Misleading action*** is when a discrepancy between information and actions available to users nudges them to do something they do not intend to. The difference between what users expect and what they get is likely to discourage them from going further.

Example 28: Users browse their social media feed. While doing so, they are shown advertisements. Intrigued by one ad and curious about the reasons it is shown to them, they click on a "?" sign available on the right bottom corner of the ad. It opens a pop-in window that explains why users see this particular ad and lists the targeting criteria. It also informs users that they can withdraw their consent to targeted advertisement and provides a link to do so. When users click on this link, they are redirected to an entirely different website giving general explanations on what consent is and how to manage it.

104. The case above exemplifies content that does not answer to users' expectations. Indeed, when users click on the link, they would expect to be redirected to a page that allows them to directly withdraw their consent. The page they are provided with instead does not allow them to do so and does not state the specific way to withdraw their consent on the social media platform. This gap between what users are supposed to find and what they actually find is likely to confuse them and leave them unsure of how to proceed. In the worst case, they could believe they cannot withdraw their consent. Such ***Misleading action*** cannot be considered transparent as required in Article 12 (1) GDPR. Additionally, comparing withdrawal with the way consent is collected, this practice could infringe Article 7 (3) GDPR if withdrawing consent turns out to be harder than giving it.

105. When social media providers inform users that an action on their part can have a certain consequence and the action actually leads to a different outcome, this constitutes ***Misleading action***, as shown in the next example.

Example 29: In the part of the social media account where users can share thoughts, pictures, etc., they are asked to confirm that they would like to share this content once they have typed it in or uploaded it. Users can choose between a button saying "*Yes, please.*" and another one saying "*No, thank you.*" However, once users decide against sharing the content with others by clicking on the second button, the content is published on their social media account.

106. As in the previous example, this information is not transparent and takes the users' choice away from them. Even though users might quickly notice the publication and delete it again, data was processed despite their refusal, and made available to others. A worse example can be found when the processing is not noticeable for users or only with difficulty or knowledge of information technology, because it takes place in the background of the social media platform.

ii. Interface-based patterns

107. Apart from the two deceptive design patterns above, it is mostly interface-based patterns that are relevant in this use case.

Skipping – Look over there (Annex I checklist 4.2.2)

108. When a data protection related action or information is put in competition with another element related or not to data protection, if users choose this other option they are likely to forget about the other, even if it was their primary intent. This is a ***Look over there*** pattern that needs to be assessed on a case-by-case basis.

> **Example 30:** A cookie banner on the social media platform states "For delicious cookies, you only need butter, sugar and flour. Check out our favourite recipe here [link]. We use cookies, too. Read more in our cookie policy [link].", along with an "okay" button.

109. Humour should not be used to misrepresent the potential risks and invalidate the actual information. In this example, users might be tempted to only click on the first link, read the cookie recipe and then click on the *"okay"* button. Apart from not providing users with a mean not to consent, this example illustrates a case where consent might not be properly informed. Indeed, by clicking on the *"okay"* button, users might think they just dismiss a funny message about cookies as baked snack and not consider the technical meaning of the term *"cookies"*. This case would not constitute informed consent in the sense of Article 7 (2) GDPR in conjunction with Article 4 (11) GDPR.

110. Article 7 (2) GDPR further states that a consent request should be clearly distinguishable from other matters. Therefore, it is necessary that the data protection information is not overshadowed by other contexts. In this example, the wordplay based on "cookie" homonyms can make the bakery context outshine the data protection context. For information to be clearly distinguishable, the relevant information for users to provide valid consent should be upfront, not ***Hidden in Plain Sight***, and not mixed with other matters or meanings. No confusion should exist between data protection information and other kinds of content. Otherwise, users might get distracted from the real implications of the processing of their personal data. When implementing these prerequisites, designers need to be given some leeway in order to make the information appealing.

Obstructing – Dead end (Annex I checklist 4.4.1)

111. Confusion or distraction is not the only effect possible with deceptive design patterns when it comes to consent. In particular, the ***Dead end*** pattern can interfere in several ways with the conditions for consent set in Article 7 GDPR in conjunction with Article 4 (11) GDPR.

> **Example 31:** Users want to manage the permissions given to the social media platform based on consent. They have to find a page in the settings related to those specific actions and wish to disable the sharing of their personal data for research purposes. When users click on the box to untick it, nothing happens at the interface level and they get the impression that the consent cannot be withdrawn.

112. In this specific example, the ***Dead end*** pattern could infringe Article 7 (3) GDPR as users are seemingly left unable to withdraw their consent to the processing of their personal data for research purposes as the mean to do so is apparently not working. If the action of the users is not properly registered within the system, a breach of Article 7 (3) GDPR can be observed. If the choice is actually registered

in the system, the fact that the interface does not reflect the users' action could be considered not respecting the principle of fairness of Article 5 (1) (a) GDPR. When an interface appears to offer the means to properly manage one's consent, by allowing users to give consent or to withdraw a previously given consent, but does not produce any visual effect when interacted with, it is misleading for the user and creates confusion and even frustration for them. Such a gap between the state the system is in and the information conveyed by the interface should be avoided as it can generally hinder users in controlling their personal data.

113. Many processing activities involve several parties, i.e. another (joint) controller or another processor being involved besides the controller or processor the data subject is in direct contact with.

> **Example 32:** A social media provider works with third parties for the processing of its users' personal data. In its privacy policy, it provides the list of those third parties without providing a link to each of their privacy policies, merely telling users to visit the third parties websites in order to get information on how these entities process data and to exercise their rights.

114. This example of the ***Dead end*** pattern shows how access to information about the respective processing is made more difficult for users. Given that they are likely not to receive all the relevant information about the processing it could be considered that such practice infringes the requirements of Article 12 (1) GDPR of easily accessible information. If such practice is used on information provided to collect consent, it can infringe the requirements of informed consent as stated in Article 7 (2) in conjunction with Article 4 (11) GDPR as information would be too difficult to reach, making data subjects not fully aware of the consequences of their choice.

Obstructing – Longer than necessary (Annex I checklist 4.4.2)

115. Article 7 (3) GDPR states that the withdrawal of consent should be as easy as giving consent. The Guidelines 05/2020 on consent under Regulation 2016/679 elaborate further on the matter by stating that giving and withdrawing consent should be available through the same mean. This entails using the same interface, but also implies that the mechanisms to withdraw consent should be easily accessible, for example through a link or an icon available at any time while using the social media platform.

> **Example 33:** A social media provider does not provide a direct opt-out from a targeted advertisement processing even though the consent (opt-in) only requires one click.

116. The time needed or the number of clicks necessary to withdraw one's consent can be used to assess if it is effectively easy to achieve. Implementing the deceptive design pattern ***Longer than Necessary*** within the user journey to withdraw their consent, as shown in example 33, goes against these principles, thus breaching Article 7 (3) GDPR.

Overloading – Privacy Maze (Annex checklist I 4.1.2)

117. As highlighted in the Guidelines 05/2020 on consent, information on the processing based on consent has to be provided to the data subjects in order for them to make an informed decision.[59] Without it, consent cannot be considered as valid. The same Guidelines further develop the ways to provide

[59] Guidelines 05/2020 on consent, para. 62-64.

information, specifying that layered information can be used to do so. However, as shown in use case 2 a,[60] social media providers need to stay mindful of avoiding the ***Privacy Maze*** deceptive design pattern when providing information related to a consent request in a layered fashion. If some information becomes too difficult to find as data subjects would need to navigate through several pages or documents, consent collected by providing such information could not be considered as informed, going against Article 7 GDPR in conjunction with Article 4 (11) GDPR. By extension, this would mean that the consent is invalid and that the social media provider would breach Article 6 GDPR.

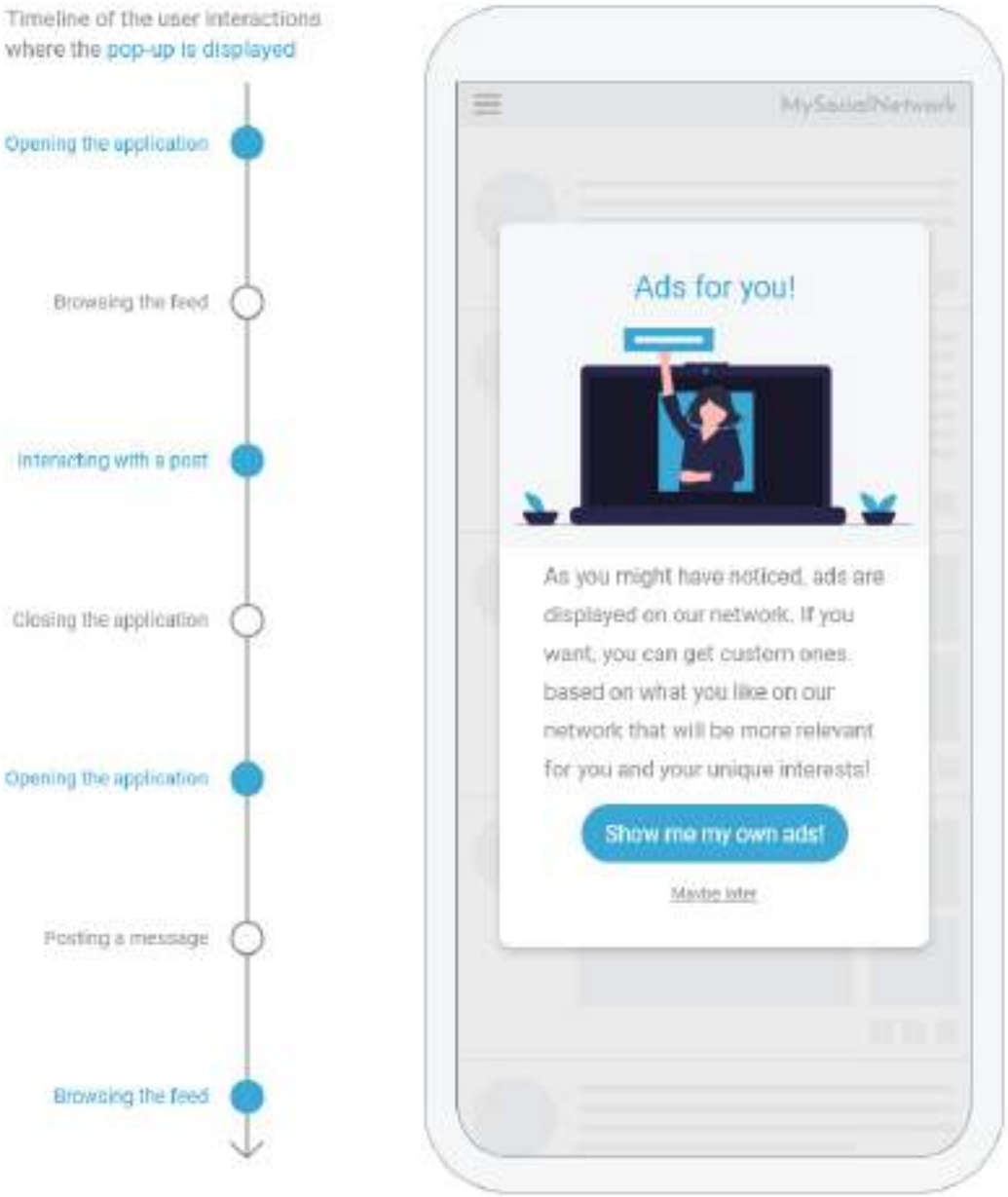
> **Example 34:** Information to withdraw consent is available from a link only accessible by checking every section of their account and information associated to advertisements displayed on the social media feed.

118. As the scenario described above shows, the deceptive design pattern ***Privacy Maze*** can also be an issue once consent is collected, by not respecting the condition under Article 7 (3) phrase 4 GDPR, which states that the withdrawal of consent shall be as easy as to give consent. This is specifically due to the fact that the process of withdrawal of consent includes more steps than the affirmative action of providing consent. As the given information is also not easily accessible to the data subject, as it is spread over different parts of the page, the principle as laid down in Article 12 (1) GDPR is violated.

Overloading – Continuous prompting (Annex I checklist 4.1.1)

119. ***Continuous Prompting***, when used on users who have not consented to the processing of their personal data for a specific purpose, creates a hindrance in the regular use of the social media. This means that users cannot refuse consent, and by extension withdraw it, without detriment. This contravenes the freely given condition for consent under Article 7 in conjunction with Article 4 (11) GDPR, that consent means any freely given indication of the data subjects' wishes by which they signify agreement to the processing of personal data relating to them. Recital 42 phrase 5 GDPR asserts further that consent cannot be considered freely given if users have no genuine or free choice. This is also supported by the EDPB Guidelines on consent, describing that consent will not be valid if data subjects have no real choice or feel compelled to consent by any element of inappropriate pressure or influence upon them, which prevents them from exercising their free will.[61] As ***Continuous Prompting*** can cause such kind of pressure, this infringes the principle of freely given consent. Additionally, as it is unlikely that once users have consented, the social media provider will regularly (e. g., every time they log back into their account) offer the possibility to withdraw consent, this deceptive design pattern can infringe Article 7 (3) phrase 4 GDPR, laying down that it shall be as easy to withdraw as to give consent ("mirroring effect").

[60] See above, para. 79-81.
[61] Guidelines 05/2020 on consent, para. 13-14.



Example 35: In this example, when users create their account, they are asked if they accept their data to be processed to get personalised advertising. In case users do not consent at sign-up to this use of their data, they regularly see – while using the social network – the prompting box illustrated above, asking if they want personalised ads. This box is blocking them in their use of the social network. Being displayed on a regular basis, this ***Continuous prompting*** is likely to fatigue users into consenting to personalised advertisement. Furthermore, in this interface the ***Hidden in plain sight*** pattern[62] is also used, as the action to accept ads is far more visible than the refusing option.

120. Additionally, the controller could infringe the principle of fairness in the sense of Article 5 (1) (a) GDPR. Given that, in the above example, users did not consent by a clear action to the processing of their personal data for targeted advertisement when creating their account, the repetitive prompting

[62] See above para. 49, or below in part 4.3.2 of the Annex.

constantly putting into question a clear refusal they made is burdensome. This clear action that users took during the registration process is now constantly put into question. The induced degradation of the user experience significantly increases the probability that users will accept the targeted advertisement at some point, just to avoid being asked again every time they log into their account and wish to use the social media platform. In this case, not giving one's consent has a direct impact on the quality of the service given to users and condition the performance of the contract.

c. Best practices

Cross-device consistency: When the social media platform is available through different devices (e.g. computer, smartphones, etc.), settings and information related to data protection should be located in the same spaces across the different versions and should be accessible through the same journey and interface elements (menu, icons, etc.).

Change spotting and comparison: see use case 1 for definition (p. 22)**.**

Coherent wordings: see use case 1 for definition (p. 22).

Providing definitions: see use case 1 for definition (p. 22).

Use of examples: see use case 1 for definition (p. 22).

Sticky navigation: see use case 2a for definition (p. 28).

Back to top: see use case 2a for definition (p. 28).

Notifications: see use case 2c for definition (p. 32).

Explaining consequences: see use case 2c for definition (p. 32).

Use case 3b: Managing one's data protection settings

a. Description of the context

121. After completing the sign-up process, and during the entire life cycle of their social media account, users should be able to adjust their data protection settings.

122. Whether users have prior knowledge of data protection in general and the GDPR in particular or not, and whether they are attentive to the personal data they do or do not wish to share and others to see, they all are entitled to being informed about their possibilities in a transparent manner while using a social media.

123. Users share a lot of personal data on social media platforms. They are often encouraged by the social media platforms to keep sharing more on a regular basis. While users might want to share moments of their life, to participate in a debate on an issue or to broaden their networks of contacts, be it for professional or personal reasons, they also need to be given the tools to control who can see which parts of their personal data. A way to avoid multiplying the number of steps required to change one's setting would be to design a privacy dashboard allowing to centralise the settings and ease the control of users' data.

b. Relevant legal provisions

124. As mentioned above,[63] as one of the main principles concerning the processing of personal data, Article 5 (1) (a) GDPR stipulates that personal data shall be processed lawfully, fairly and, especially crucial in this regard, in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency"). According to the accountability principle as per Article 5 (2) GDPR, controllers are required to show which measures they are taking to make their processing activities not only lawful and fair, but also transparent. In addition, the principles of minimisation under Article 5 (1) (c) and data protection by design and default under Article 25 GDPR are relevant in this use case.

c. Deceptive design patterns

i. Content-based patterns

125. The first issue that users encounter in this context is where to actually find settings dealing with data protection. Users might read the data protection notice and then decide to make changes related to the processing of their personal data. They could also wish to do so without having read the notice, just through their regular use of the social media, for example when they realise that an information posted on a social media platform (e.g. a photo at the beach with one's family) is shared with an undesired group of people (e.g. co-workers). In any event, the principle of transparency requires the setting options to be easily accessible as well as to be available in an understandable way. This could be achieved by centralising the data and privacy settings in one place using a self-explanatory URL such as [social-network.com]/data-settings.

126. There are several design patterns related to this issue which make it hard for users to find the settings. Social media platform designers therefore ought to be mindful to avoid these deceptive design patterns.

Overloading – Too many options (Annex I checklist 4.1.3)

127. Data protection settings need to be easily accessible and ordered logically. Settings related to the same aspect of data protection should preferably be located in a single and prominent location. Otherwise, users will be facing too many pages to check and review which overburdens them in the settings of their data protection preferences. Indeed, confronted with ***Too many options*** to choose from, it can leave them unable to make any choice or make them overlook some settings, finally giving up or missing the settings of their data protection preferences. This infringes the principles of transparency and fairness. In particular, it can infringe Article 12 (1) GDPR as it either makes a specific control related to data protection hard to reach as it is spread across several pages or makes the difference between the different options provided to users unclear.

> **Example 36:** Users are likely to not know what to do when a social media platform's menu contains multiple tabs dealing with data protection: "*data protection*", "*safety*", "*content*", "*privacy"*, "*your preferences*".

128. In this example, the tab titles do not obviously indicate what content users can expect on the associated page or that they all relate to data protection, especially when one of the tab specifically bears this name. This can create the risk of preventing users from making changes. For example, if they would like to restrict or broaden the number of persons who can see the pictures they have uploaded, the tab names could lead them to either click on "safety", if users think there are some safety risks in

[63] See above, para. 1, 9, 10, 14-16.

having their data publicly accessible; "content", as users wish to set the visibility of their post; or "privacy", as this specific notion directly relates to what people want to share with others. This means that these titles are not clear enough in regard of the action users would like to achieve. In particular, the terms "data protection" and "privacy" are often used as synonyms and are therefore especially confusing if presented as different sections.

Left in the dark – Conflicting information (Annex I checklist 4.6.2)

129. As already described in example 12 and further illustrated in the following example, users can also be given ***Conflicting information*** within the framework of the data protection settings.

> **Example 37:** User X switches off the use of their geolocation for advertisement purpose. After clicking on the toggle allowing to do so, a message appears saying *"We've turned off your geolocation, but your location will still be used."*

Overloading – Privacy maze (Annex I checklist 4.1.2)

130. 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. If such settings are spread across different, unconnected pages of the social media platform, users are likely to miss one or several means to control an aspect of their personal data. Users expect to find related settings next to each other.

> **Example 38:** Related topics, such as the settings on data sharing by the social media provider with third parties and vice versa, are not made available in the same or close spaces, but rather in different tabs of the settings menu.

131. There is no "one size fits all approach" when it comes to the average number of steps still bearable for users of social media platforms to take when changing a setting. At the same time, a higher number of steps can discourage users from finalising the change or make them miss parts of it, especially if they want to make several changes. Hindering in such a way the will of users infringes the principles of fairness in Article 5 (1) (a) GDPR. In addition, changing the settings is closely related to the exercise of data subject rights.[64] Changing a data related setting, such as correcting one's name or deleting one's graduation year, can be considered an exercise of the right to rectification, respectively right to erasure, for these specific data. The number of steps required should therefore be as low as possible. While it might vary, an excessive number of steps hinders users and therefore infringes the fairness principle, as well as Articles 12 (1) and (2) GDPR.

Fickle – Language Discontinuity (Annex I checklist 4.5.4)

132. With regard to transparent information, social media platform designers also need to be careful to avoid content-based deceptive design patterns listed in use case 2a, such as ***Language discontinuity***. Not making the setting pages (or parts of them) available in the language users chose for the social media platform makes it harder for them to understand what they can change and therefore set their preferences.

[64] See below, Use cases 4 and 5, i.e. parts 3.4. and 3.5. of these Guidelines.

Fickle – Inconsistent Interface (Annex I checklist 4.5.3)

133. In this context, another issue occurs when social media platforms offer data protection friendly choices to users, but do not inform them about it in a clear manner. This can be the case when the social media platform suddenly differs from its usual design pattern. Such an ***Inconsistent Interface*** occurs when an interface is not consistent across different contexts or with users' expectations. These differences can lead users not to find the desired control or information or to interact with an element of the interface out of habits even though this interaction leads to make a data protection choice the users do not want.

> **Example 39:** Throughout the social media platform, nine out of ten data protection setting options are presented in the following order:
>
> - most restrictive option (i.e. sharing the least data with others)
>
> - limited option, but not as restrictive as the first one
>
> - least restrictive option (i.e. sharing the most data with others).
>
> Users of this platform are used to their data protection settings being presented in this order. However, this order is not applied at the last setting where the choice of visibility of users' birthdays is instead shown in the following order:
>
> - *Show my whole birthday: 15 January 1929* (= least restrictive option)
>
> - *Show only day and month: 15 January* (= limited option, but not the most restrictive one)
>
> - *Do not show others my birthday* (= most restrictive option).

134. In the example, the three choices in the last setting are presented in a different order than the previous settings. Users who have previously changed their other settings are likely to be used to the "usual" order of settings one to nine. At the last setting, they are so used to this order that they instinctively choose the first option, assuming that this must be the most restrictive one. Arranging the options of one data protection setting so differently from the others in the same social media platform is an ***Inconsistent Interface*** as it plays with what users are used to and their expectations. This can lead to confusion or leave users to think they took the choice they wanted when, in reality, this is not the case.

ii. Interface-based patterns

135. The second issue one encounters in the context of data protection settings is that the settings might infringe on the principle of data protection by default. Article 25 (1) GDPR requires controllers to take appropriate measures designed to implement data protection principles, such as data minimisation (Article 5 (1) (c) GDPR). These provisions are not respected when the settings on sharing of personal data are pre-set to one of the more invasive options rather than the least invasive one.

Skipping – Deceptive Snugness (Annex I checklist 4.2.1)

> **Example 40:** Between the data visibility options *"visible to me", "to my closest friends" "to all my connections",* and *"public"*, the middle option *"to all my connections"* is pre-set. This means that all users connected to them can see their contributions, as well as all

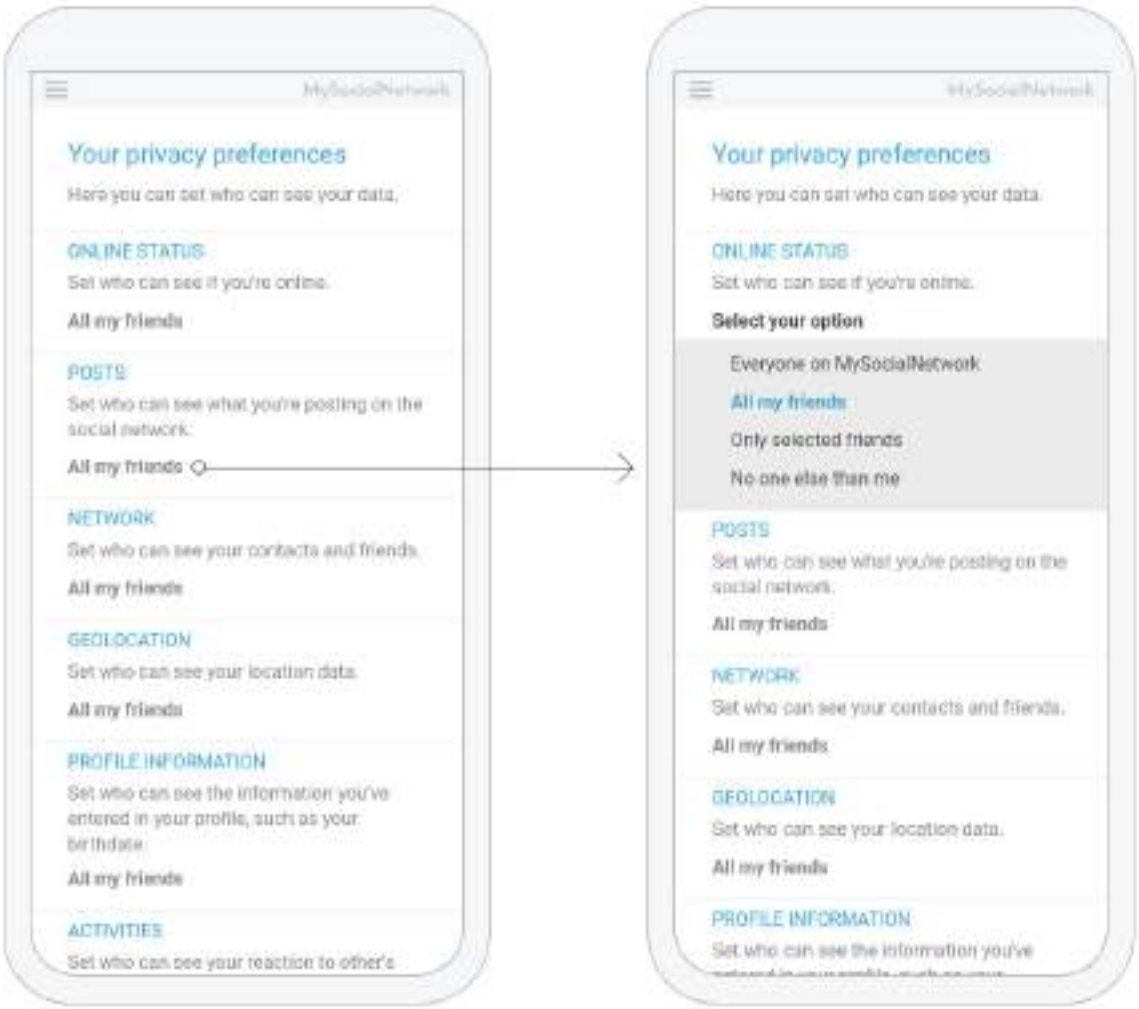
information entered for signing-up to the social media platform, such as their email address or birthdate.

136. Social media providers might argue that the least invasive setting would defeat the goal that users of a particular social media platform have, for example being found by unknown people to find a new buddy, date or job. While this might be true for some particular settings, social media providers need to keep in mind that the fact that users upload certain data on the network does not constitute consent to share this data with others.[65] Where social media providers defer from data protection by default, they will need to be mindful to properly inform users about it. This means that users need to know what the default setting is, that there are less invasive options available and where on the platform they need to go to make changes. In the given example, it means that when the option "*to my closest friends*" is pre-set for contributions users actively post on the social media platform, they should be shown where to change this setting. However, pre-setting the visibility to "*all user connections*" (or even the general public) constitutes ***Deceptive Snugness****,* especially when it is applied to data the social media provider required from users to create an account, such as the email address or their birthdate. As described in use case 1 para. 55, this practice infringes Article 25 (2) GDPR.

[65] For example their birthdate, see para. 58 above.

Stirring – Hidden in plain sight (Annex I checklist 4.3.2)

137. The ***Hidden in Plain Sight*** and ***Deceptive Snugness*** deceptive design patterns can easily be combined when it comes to the selection of data protection related options as illustrated in example 9 for the sign-up process, and below when users want to change their data protection preferences while using the social media.



Example 41: In this example, when users want to manage the visibility of their data, they have to go in the *"privacy preference"* tab. The information for which they can set their preference is listed there. However, the way that information is displayed does not make it obvious how to change the settings. Indeed, users have to click on the current visibility option in order to access a dropdown menu from which they can select the option they prefer.

138. Even though changing one's preferences is available in this tab, it is ***Hidden in plain sight*****,** as the dropdown menu is not directly visible for users who have to guess that clicking on the current option will open something. There is indeed no usual visual clue (underlined text, down arrow) about the possibility of interacting and opening the dropdown menu. This specific practice is unfair to users and could participate in a general failure to meet the principle of fairness of Article 5 (1) (a) GDPR. Additionally, if the options were pre-selected by default, the deceptive design pattern ***Deceptive Snugness*** could be also observed, as described above in para. 128.

Fickle – Decontextualising (Annex I checklist 4.5.2)

139. ***Decontextualising*** happens when a data protection related information or control is located on a page that is out of context, so that users are unlikely to find it as it would not be intuitive to look for it on that specific page.

> **Example 42:** The data protection settings are difficult to find in the user account, as on the first level, there is no menu chapter with a name or heading that would lead in that direction. Users must look up other submenus such as "*Security*".

140. In this example, users are not guided to the data protection settings because no meaningful and clear terms are used to indicate where these are on the social media platform. Indeed, the term *"Security"* only covers a fraction of what can be expected of data protection settings. It is therefore not intuitive for users to look up this menu to find such settings. This lack of transparency makes access to information harder than it should and can be considered as contravening Article 12 (1) GDPR, and potentially Article 12 (2) GDPR if those settings relate to the exercise of a right.

> **Example 43:** Changing the setting is hindered since in the social media platform's desktop version, the "*save*" button for registering their changes is not visible with all the options, but only at the top of the submenu. Users are likely to overlook it and wrongly assume their settings are saved automatically, therefore moving to another page without clicking on the "*save*" button. This problem does not occur in the app and mobile versions. Therefore, it creates additional confusion for users moving from the mobile/app to the desktop version, and can make them think they can only change their settings in the mobile version or the app.

141. Once users have found the data protection settings and set their choices, they may not be hindered from doing so. Once users have made a change, the way to save it has to be obvious, whether this happens as soon as users adjust a setting or it needs a confirmation by clicking on a specific element of the interface such as a "save" button. In addition, the principle of fairness under Article 5 (1) (a) GDPR requires social media providers to be consistent throughout their platform, especially across different devices. That is not the case when the interface uses a deceptive design pattern as described in the examples above.

d. Best practices

Data protection directory: For easy orientation through the different section of the menu, provide users with an easily accessible page from where all data protection related actions (e. g., settings) and information are accessible. This page could be found in the social media provider main navigation menu, the user account, through the privacy policy, etc.

Bulk options: Putting options that have the same processing purpose together, so that users can change them more easily, while still leaving users the possibility to make more granular changes. If social media platforms present bulk options, these should not contain unexpected or unrelated elements (for example elements with different purposes). If the processing require consent, the bulk options must be in line with the EDPB Guidelines on consent, especially para. 42-44.

Shortcuts: see use case 1 for definition (p. 22) *(e.g. when users are informed about an aspect of the processing, they are invited to set their related data preferences on the corresponding setting/dashboard page)***.**

Self-explanatory URL: pages related to data protection settings or information should use a web address that clearly reflects their content. For example, a page centralising data protection control could have a URL such as [social-network.com]/data-settings.

Coherent wordings: see use case 1 for definition (p. 22).

Providing definitions: see use case 1 for definition (p. 22).

Use of examples: see use case 1 for definition (p. 22).

Sticky navigation: see use case 2a for definition (p. 28).

Notifications: see use case 2c for definition (p. 32).

Explaining Consequences: see use case 2c for definition (p. 32)**.**

Cross-device consistency: see use case 3a for definition (p. 39).

3.4 Staying right on social media: Data subject rights

Use case 4: How to provide proper functions for the exercise of data subject rights

a. Description of the context

142. Using a social media platform means taking advantage of its functions along the purposes stated by the social media provider. This also means for users to be able to exercise their data protection rights. They are key elements of data protection and controlling one's own information, regardless of whether data are directly and knowingly provided by data subjects, provided by data subjects by virtue of the use of the service or the device, or inferred from the analysis of data provided by the data subject.[66] The amount of personal data flowing throughout the platform requires enabling users to control their data with the help of the rights provided by the GDPR in a clear and intuitive manner. The EDPB has explained these concepts in several guidelines.[67] The exercise of rights must be available from the beginning until the end of using the platform, and in some cases, even after users have decided to leave the platform and the controller has not yet deleted their data. Non-users of the platform also need to be enabled to exercise data subject rights pertaining to processing of their data. Of course, in some instances not all the data subject rights are available depending on the legal basis for processing the data. The social media provider should therefore also clearly explain why certain rights are not applicable and why some of them may be limited. As mentioned above and in previous chapters the use of rights must be made operative. Automation as well as other functionalities of social media platforms should be used to facilitate the exercise of rights.

b. Relevant legal provisions

143. The GDPR describes seven different rights that data subjects can exercise according to certain conditions (e.g. legal basis of the processing, etc.). Article 15 GDPR allows data subjects to know if

[66] See Article 29 Working Party Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01, p. 10, https://ec.europa.eu/newsroom/article29/items/611233/en.

[67] Guidelines on the right to data portability and EDPB Guidelines 05/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) - version adopted after public consultation, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en.

personal data concerning them are processed and to access them, i.e. to obtain further information on their processing, as well as to receive a copy of that data. Article 16 GDPR details the right to rectification allowing data subjects to update the personal data the controller processes. The right to erasure under Article 17 GDPR allows data subjects to obtain the erasure of personal data concerning them. The right to restriction of processing under Article 18 GDPR gives the data subjects the possibility to stop temporarily the processing of their personal data. Article 20 GDPR introduces the right to data portability allowing data subjects to receive their personal data and transmit it to another controller.[68] Data subjects have also the right to object to the processing of their personal data as laid out in Article 21 GDPR. Finally, Article 22 GDPR gives data subjects the right not to be subject of a decision based solely on automated processing.[69]

144. The EDPB underlines that not all of these rights will apply to every social media platform, depending on its legal basis and purposes of processing of personal data and types of services provided. The differences should be explained by the controller in accordance with Article 12 GDPR. This means that the information on applicable rights should be concise and clear to users, including why certain rights do not apply. Such an explanation could limit the amount of communication with users when they are trying to exercise some of them. The exercise of the right should be easy and accessible in accordance with Article 12 (2) and the reply should be given without undue delay as required per Article 12 (3) GDPR. Similarly, the social media platform should explain why certain requests cannot be fulfilled and inform on the possibility to lodge a complaint to a designated supervisory authority as per Article 12 (4) GDPR. Thus, the following deceptive design patterns may not be applicable to all of the rights mentioned above. The right to erasure is discussed in detail in the next chapter.

c. Deceptive design patterns

i. Content-based patterns

Obstructing – Dead end (Annex checklist I 4.4.1)

145. The ***Dead end*** deceptive design pattern can directly impact the ease of access to the exercise of the rights. When links redirecting to the means to exercise a right are broken or clear explanations on how to exercise a right are missing, users will not be able to properly exercise it, which infringes Article 12 (2) GDPR.

> **Example 44:** Users click on "*exercise my right of access*" in the privacy notice, but are redirected to their profile instead, which does not provide any features related to exercising the right.

146. The above-mentioned example of a deceptive design pattern outlines the need to provide users with a clear and intuitive manner to exercise their rights in accordance with Article 12 (1) and (2) GDPR, as they might otherwise not be able to exercise them. It is not enough to confirm to users that they have data subject rights as required per Article 12 (1) GDPR (including the manner of communication) and specifically per Articles 13 (2) (b) and 14 (2) (c) GDPR. Users must also be able to easily exercise them, preferably in a way embedded in the platform's interface, for example by providing a dedicated form. This would also make the user experience with a platform more positive – seeing that the provider has taken the effort to adapt to users' expectation of lawful personal data processing and control over

[68] This right is further developed in the Guidelines on the right to data portability.
[69] See also Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, wp251rev.01, p. 19 and following, https://ec.europa.eu/newsroom/article29/items/612053/en.

their data by combining the exercise of rights with other functionalities of the service. When the social media platform service allows for a two-way communication among users, as well as between the controller and users, there is no reason for the controller to limit its channel of communication for the facilitation of data subject requests to a separate mean of communication like email. At the same time, data subjects should not be forced to come to the platform to communicate with the controller.[70] In addition, controllers may not limit this data subject right to the right to copy, but instead need to make sure they also provide the information mentioned by Article 15 (1) GDPR to users requesting access to their data.[71]

Fickle – Language discontinuity (Annex I checklist 4.5.4)

> **Example 45:** When clicking on a link related to the exercise of data subject rights, the following information is not provided in the state's official language(s) of the users' country, whereas the service is. Instead, users are redirected to a page in English.

147. Bearing in mind the principle of transparency under Articles 5 (1) (a) and 12 (1) GDPR, users must receive all the information about their rights in a clear and plain, comprehensible manner. This must also be related to users' location and the language used in that country or jurisdiction in which the service is offered. The fact that users confirm their ability to use a foreign language in any way does not release the controller from its obligations. The same applies when such knowledge of other languages understood by the users can be inferred from their activities. The information should be relevant and helpful to users exercising their rights.

Left in the dark – Ambiguous wording or information (Annex I checklist 4.6.3)

148. In the context of data subject rights, users can also be confronted with the deceptive design pattern ***Ambiguous wording or information***, as shown in the following example.

> **Example 46:** The social media platform does not explicitly state that users in the EU have the right to lodge a complaint with a supervisory authority, but only mentions that in some – without mentioning which – countries, there are data protection authorities which the social media provider cooperates with regarding complaints.

149. Social media providers also need to be mindful to avoid the ***Ambiguous wording or information*** deceptive design pattern when informing data subjects about their rights. Giving information to users in a way that makes them unsure of how their data will be processed or how to have some control over their data and thus how to exercise their rights infringes the principle of transparency. Additionally, vague wording is not concise language as required by Article 12 (1) GDPR and can make the information provided to the data subject incomplete, which could be considered a breach of Article 13 GDPR. The above-mentioned example also shows an infringement of Article 13 (2) (d) GDPR which requires controllers to provide data subjects with information about their right to lodge a

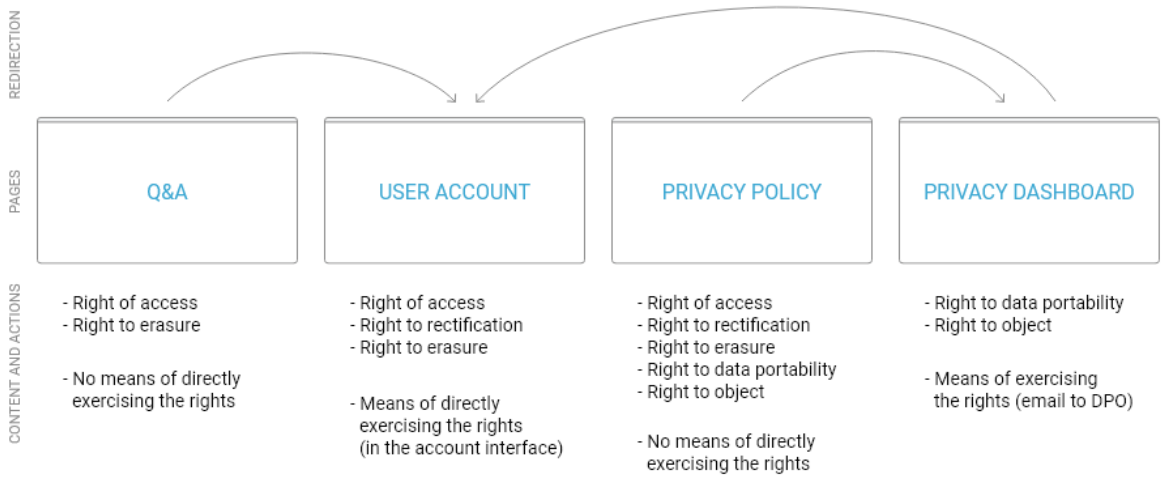
[70] See EDPB Guidelines 01/2022 on data subject rights – right of access, para. 136, version 1.0, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.
[71] See EDPB Guidelines 01/2022, para. 131, 142, 145.

complaint with a supervisory authority. By extension, this is also contrary to Article 12 (2) GDPR because the social media provider does not facilitate the exercise of the right to lodge a complaint.

ii. Interface-based patterns

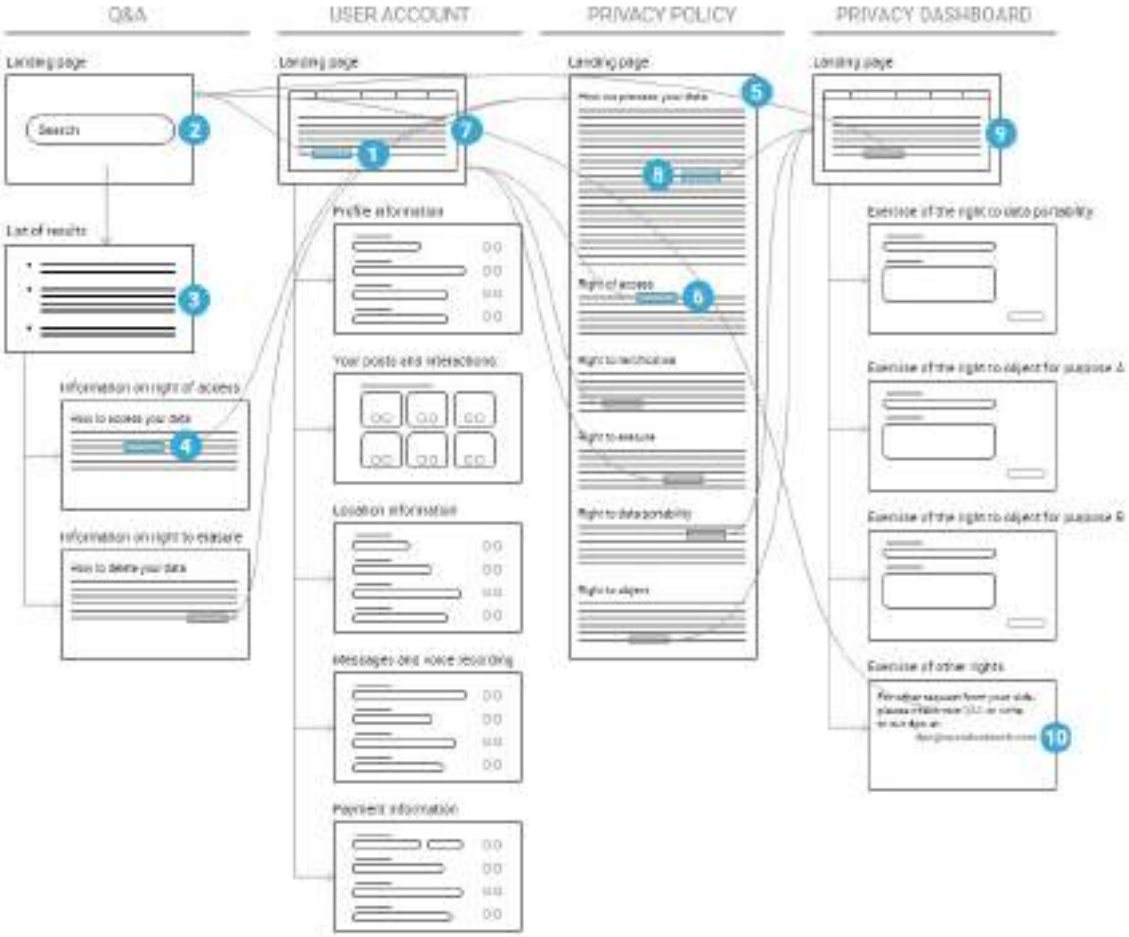
Overloading – Privacy Maze (Annex I checklist 4.1.2)

150. As described earlier in use case 3b, the number of steps necessary to receive the relevant data protection information shall not be excessive, and neither may the number of steps to achieve the data subject rights.[72] Thus, users should always be able to reach the rights exercise site quickly, no matter which starting point they came from and where the social media platform has located this feature. Social media providers should therefore think carefully about the different situations from which users would like to exercise their rights and design access to the place where they can do so accordingly. This means that several paths to reach a data subject right can be created and available on a social media platform. However, each path should facilitate the access to the exercise of the rights and should not interfere with another path. If not, it would be considered to be a ***Privacy Maze*** deceptive design pattern, as illustrated in examples 47 and 48, contrary to Article 12 (2) GDPR.



Example 47: Here, information related to data protection rights is available on at least four pages. Even though the privacy policy informs on all the rights, it does not redirect to the relevant pages for each of them. Conversely, when users visit their account, they will not find any information on some of the rights they can exercise. This ***Privacy Maze*** forces users to dig through many pages in order to find where to exercise each right and, depending on their browsing, they might not be aware of all the rights they have.

[72] See above, para. 123.



Example 48: In this example, users wish to update some of their personal data but do not find a way to do it in their account. They click on a link (1) redirecting them to the Question & Answer page where they enter their question (2). Several results appear (3), some related to the rights of access and deletion. After checking all results, they click (4) on the link available in the "How to access your data" page. It redirects them to the privacy policy (5). There, they find information on additional rights. After reading this information, they click (6) on the link associated with the exercise of the right to rectification which redirects them to the user account (7). Unsatisfied, they go back to the privacy policy and click on a general link "Send us a request" (8). This brings users to their privacy dashboard (9). As none of the available options seem to match their need, users eventually go to the "exercise of other rights" page (10) where they finally find a contact address.

151. Both examples illustrate particularly lengthy and tiresome paths to exercise one's rights. When the means of exercising different rights are not located in the same space but a page listing all the data subject rights is available, the latest should redirect precisely to those different spaces, not only to one or part of them as illustrated in example 47. The other example shows a journey where users do not find the mean to easily exercise the specific right they wish, namely the right to rectification, as the place where it is commonly carried out, namely the user account, does not provide the mean to do so.

Looking for another way to exercise this right, they cannot find a specifically corresponding one and have to turn to a general mean provided in the privacy dashboard.

152. When several paths to the exercise of a right have been designed, it should always be easy for users to find the overview about the data subject rights. Privacy policies should be clear and could serve as one of the gateways to pages where users can exercise their rights. This document should include all of the rights that are applicable. If any of them should be unavailable due to legal or technical limitations this should also be explained, so that users are informed properly. Understanding the limitations of processing operations, either due to their basis or safeguards adopted by controllers, is helpful not only to users. It also limits the instances in which a social media provider has to explain why it cannot comply with a data subject rights request made by users.

Stirring – Hidden in plain sight (Annex I checklist 4.3.2)

153. Affecting users' ability to reach the place where to exercise their right can also be done by making related information or links hardly visible using the ***Hidden in Plain Sight*** deceptive design pattern.

> **Example 49:** The paragraph under the subtitle "right to access" in the privacy policy explains that users have the right to obtain information under Article 15 (1) GDPR. However, it only mentions users' possibility to receive a copy of their personal data. There is no direct link visible to exercise the copy component of the right of access under Article 15 (3) GDPR. Rather, the first three words in "You can have a copy of your personal data" are slightly underlined. When hovering over these words with the users' mouse, a small box is displayed with a link to the settings.

154. Adding to the previous section, any means created by the controller for the exercise of rights should be easily accessible. This rule cannot be understated. An action by the controller as described above can be viewed only as an effort to hinder the exercise of rights by users, which infringes Article 12 (2) GDPR. Controllers, no matter their reasons, should not inhibit such a request. Upon closer examination by a supervisory authority in a specific case this could contribute to a breach of GDPR leading to sanctioning the controller.

Fickle – Inconsistent Interface (Annex I checklist 4.5.3)

> **Example 50:** The social media platform offers different versions (desktop, app, mobile browser). In each version, the settings (leading to access/objection etc.) are displayed with a different symbol, leaving users who switch between versions confused.

155. Confronted with interfaces across different devices that convey the same information through various visual signifiers, users are likely to take more time or have difficulties finding controls they know from one device to another. In the example above, this is due to the use of different symbols or icons to direct users to the settings. Confusing users in such a way could be considered conflicting with the facilitation of data subject rights as stated in Article 12 (2) GDPR.

Obstructing – Longer than necessary (Annex I checklist 4.4.2)

156. Finally, any attempt to make the exercise of a right ***Longer than Necessary*** can be considered contrary to the GDPR.

> **Example 51:** When users choose to delete the name and place of their high school or the reference to an event they attended and shared, a second window pops up asking to confirm that choice ("*Do you really want to do so? Why do you want to do this?")*.

157. Similarly to the amount of layers in a privacy policy (use case 2a) and the number of steps to reach or change a setting (use case 3b), the amount of steps or clicks users need to take to exercise a right should not be excessive. This of course depends on the complexity of operations conducted by the controller taking into consideration the specific context. It would however be unreasonable to require users to take a high number of unnecessary actions in order to finish exercising their right. For example, users should not be discouraged by additional questions, such as whether they really want to exercise this right or what the reasons for such a request are. In most cases they should be able to just exercise their right, without their motivation being put into question. Such practices, illustrated in the example above, can be considered contrary to Article 12 (2) GDPR as the controller hinders the exercise of the rights with unnecessary steps. This of course does not preclude the controller from receiving feedback by asking additional questions afterwards for the purpose of making the service better. By asking this question afterwards, answering it would depend solely on the users' will and would not be mistaken for a requirement to exercise a right.

d. Best practices

Exercise of the rights form: to facilitate users in exercising their GDPR rights, provide a dedicated form that helps users understand their rights and that guides them carry out these kind of requests.

Shortcuts: see use case 1 for definition (p. 22) (e.g. *provide a link to account deletion in the user account*)**.**

Coherent wordings: see use case 1 for definition (p. 22).

Providing definitions: see use case 1 for definition (p. 22).

Use of examples: see use case 1 for definition (p. 22).

Sticky navigation: see use case 2a for definition (p. 28).

Explaining Consequences: see use case 2c for definition (p. 32)**.**

Cross-device consistency: see use case 3a for definition (p. 39).

Data protection directory: see use case 3b for definition (p. 45).

Data protection controls relation: see use case 3b for definition (p. 45).

3.5 So long and farewell: leaving a social media account

Use case 5: pausing the account/erasure of all personal data

a. Description of the context and relevant legal provisions

158. The end of the life cycle of an account describes the situation when users decide to leave the social network. In this situation, users usually decide to leave the social media platform permanently. However, there is often also the option of only temporarily disabling the account and pausing the service. The legal implications of both decisions differ and are described below.

i. Permanent erasure of the account

159. 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.

160. The word "erasure" is not legally defined in Article 17 GDPR and is only mentioned as a form of processing in Article 4 (2) GDPR. Erasure can be generally understood as a (factual) impossibility to perceive the information about a data subject previously embodied in the data to be erased. After erasure, it must no longer be possible for anyone to perceive the information in question without disproportionate effort.

161. Anonymisation is another way of permanently removing the relation to a person. In other words, the use of anonymisation techniques is intended to ensure that the data subject can no longer be identified. Anonymisation also means that the principles of data protection law – such as the principle of purpose limitation – are no longer applicable (see Recital 26, phrases 4 and 5).

162. According to Article 12 (2) GDPR, the controller shall facilitate the exercise of data subject rights under Articles 15 to 22. According to this requirement, no substantive or formal hurdles may be created in the assertion of data subject rights. Therefore, if the exercise of the right of erasure is made more difficult without actual reason, this constitutes a violation of the GDPR. While there is a valid reason for social media providers objectively explain the consequences, such as deletion of all personal data, and ask data subjects to confirm this choice,[73] unnecessary hurdles also need to be avoided in this use case. From this follows e.g. that any grace period between users' account deletion requests and the actual deletion of the account needs to be proportionate. Thus, such a time may not be excessive, taking into account necessary technical reasons for delays from immediate deletion, as well as a short time for users' (re-)consideration about deleting their account once they have triggered the account deletion process. While users' free will to change their mind needs to be respected, social media providers may not try to trigger such a change of mind by inciting users to come back, which would also constitute a hindrance of users' right to deletion. During the grace period, the deletion process could be interrupted in some cases, e.g. when the user logs in again. If the deletion cannot be completed, the user must be informed and instructed on how to complete the deletion.

163. The decision to leave the social media platform triggers the consequences of erasure as stated in Article 17 (1) GDPR. If a data subject requests the deletion of the respective account, the controller of a social media platform needs to delete the data. Nevertheless, some data can remain with the social media platform for a certain period of time if Article 17 (3) GDPR is applicable. The exceptions listed in Article 17 (3) GDPR have to be interpreted narrowly and only apply in the cases explicitly named in this part of the provision. Any exception that a controller relies on under Article 17 (3) GDPR and the respective retention of data need to be justified by the controller, e. g., that national law requires the controller to store information related to the data subject for overriding reasons of public interest, for

[73] Contrary to the other data subject rights, see para. 154 above.

exercising the fundamental right of freedom of expression and information or for tax reasons. It goes without saying that such remaining data should only be stored internally by the Social Media Provider and should not be publicly visible for other users. In no way, however, does an exemption under Article 17 (3) GDPR enable the social media provider to keep running the account of the data subject longer than intended by the users after their request for deletion.

164. Independently of a request to delete the account, if users withdraw their consent under Article 7 (3) GDPR, processing of their consent-based provided data under Article 6 (1) (a) GDPR may no longer take place. In this case, other processing operations where the social media provider relies on other legal bases under Article 6 (1) GDPR may, under certain circumstances, still take place.

165. If users ask, however, to delete their account, no further processing should take place, irrespective of the underlying legal basis, unless one of the exceptions exhaustively listed in Article 17 (3) GDPR applies. In this context, it is important to keep in mind that retention is limited to the above-mentioned minimal storage

166. According to Article 25 (1) GDPR, the controller shall implement appropriate technical and organisational measures to put the data protection principles into practice. According to the Guidelines 04/2019 on Article 25 – Data Protection by Design and by Default, technical and organisational measures can be understood in a broad sense as any method or means that a controller may employ in the processing. Being appropriate means that the measures should be suited to achieve the intended purpose, i.e. they must implement the data protection principles effectively. The requirement to appropriateness is thus closely related to the requirement of effectiveness.[74]

[74] Guidelines 04/2019 on Article 25 Data Protection by Design and by Default, page 6, para. 8.

ii. Pausing the account

167. Alternatively, users are offered the opportunity to temporarily deactivate their account which allows users to leave the social media for a period of time without deleting their account permanently. In this case, the account is temporarily disabled and the profile, pictures, comments and reactions will be hidden until users reactivate their account, e. g. by logging back in. The main difference to the erasure is that the personal data remain with the social network and the account can be re-activated by users without a new registration.

168. Users starting the process to delete their account may find that the option to pause the account instead is pre-selected. While it might be useful for users who would not like to permanently delete their account just yet to be offered a pausing option, social media providers may not impose such cooling-off periods on users, especially through pre-selection. By offering the possibility of deactivation, the social media provider raises users' reasonable expectations that their personal data will not be processed in the same manner as during the active use of the account and that the social media provider reduces the processing of personal data to a strictly necessary level during this period. Users might expect that their data are not or not fully processed for specific purposes, e.g. by enhancing their profile with visits to third party websites that use appropriate targeting or tracking tools. In addition to informing users in a transparent manner about the consequences of pausing their account, any processing of data taking place during this pause needs to rely on a valid legal basis.

169. In respect of data processing relying on consent according to Article 6 (1) (a) GDPR, the social media provider must take into account that users expect that the consent they give during the registration or afterwards only covers data processing during their active use of the account. The EDPB recognises that the duration of consent depends on the context, the scope of the initial consent and the expectations of the data subject.[75] Although there is no specific time limit in the GDPR for how long consent will last, the validity will depend on the context, the scope of the original consent and the expectations of the data subject.[76] If the processing operations change or evolve considerably, then the original consent is no longer valid.[77] The EDPB recommends as a best practice that consent should be refreshed at appropriate intervals.[78] Providing all the information again helps to ensure that data subjects remain well informed about how their data is being used and how to exercise their rights.[79] If this is the case, consent needs to be obtained again[80] and all corresponding requirements must be fulfilled.

170. The reasonable expectations of the data subject should also be taken into consideration when Article 6 (1) (f) GDPR is applicable (see Recital 47). In particular, it is necessary to consider whether the data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may be taking place. However, users reasonably expect that only necessary data processing will take place during the time of deactivation. Moreover, the social media provider can only rely on legitimate interest if all steps of the legitimate interest test, including the balancing exercise are met. Any overriding interest or fundamental rights and freedoms of the data subject should be assessed on a case-by-case basis.

[75] Guidelines 5/2020 on consent, para 110.
[76] Guidelines 5/2020 on consent, para 110.
[77] Guidelines 5/2020 on consent, para 110.
[78] Guidelines 5/2020 on consent, para 111.
[79] Guidelines 5/2020 on consent, para 111.
[80] See Guidelines 5/2020 on consent, para 110.

171. Since contractual obligations are also suspended to a large extent during the deactivation, data processing operations are only necessary to a limited extent under Article 6 (1) (b) GDPR. Only the storage of users' data until the final decision on reactivation or deletion can be regarded as necessary.

172. In view of the fact that all previous data processing was aimed at an active account, additional information about the processing during the deactivation must be provided if it is not included in the general information under Articles 13, 14 GDPR. This follows from the principles of transparency and fairness under Article 5 (1) (a) GDPR and purpose limitation from Article 5 (1) (b) GDPR. The data processing following deactivation must be accompanied by sufficient information of the data subject. Therefore, the social media provider shall comprehensively inform users about the actual processing and its purposes during the pause and, if necessary, obtain new consent.

b. Deceptive design patterns

i. Content-based patterns

Overloading – Privacy Maze (Annex I checklist 4.1.2)

173. In this use case, the deceptive design pattern ***Privacy maze*** occurs when users are buried under a mass of information, spread across several places, to keep them from deleting their account, as the example below shows. While some additional information before this step is quite desirable, such as the indication that users have access to their data before deletion, general unrelated information is no longer crucial. Users should not be unnecessarily delayed in taking this step.

> **Example 52:** Users are looking for the right to erasure. They have to call up the account settings, open a sub-menu called “privacy”, and have to scroll all the way down to find a link to delete the account.

Stirring – Emotional Steering (Annex I checklist 4.3.1)

> **Example 53:** On the first information level, information is given to users highlighting only the negative, discouraging consequences of deleting their accounts (e.g. *"you'll lose everything forever"* or *"your friends will forget you"*).

174. Whereas regret over the termination of contractual relationship appears socially adequate and is therefore difficult to capture in legal terms, a comprehensive description of the supposedly negative consequences caused by users erasing their account constitutes an impediment against their decision if done as in the example above which plays with the fear of missing out (FOMO), making the choice of deleting one’s account look like particularly punishing. Such ***Emotional steering***, threatening users that they will be left alone if they delete their account, constitutes an infringement of the obligation to facilitate the exercise of data subject rights under Article 12 (2) GDPR, as well as of the principle of fairness under Article 5 (1) (a) GDPR.

Left in the dark – Ambiguous wording or information (Annex I checklist 4.6.3)

175. In the context of deleting a social media account, users can also be confronted with the deceptive design pattern ***Ambiguous wording or information***, as shown in the following example.

> **Example 54:** When users delete their account, they are not informed about the time their data will be kept once the account is deleted. Even worse, at no point in the whole deletion

process users are advised about the fact that "*some of the personal data"* might be stored even after deleting an account. They need to look for the information by themselves, across the different information sources available.

Example 55: Users can only delete their account through links named *"See you"* or *"Deactivate"* available in their account.

176. In these examples, the wording used for the links does not clearly convey the fact that users will be redirected to the account deletion process. Instead, users are likely to think of other functionalities such as logging off until the next use, or deactivation of their account. As such, this could be interpreted as an infringement of Article 12 (2) GDPR stating that data controllers should facilitate the exercise of the rights of data subjects. By creating confusion on the expectations of users associated with the link, the social media platform does not fully facilitate the exercise of the right of erasure. The use of such equivocal words in other context could infringe GDPR provisions such as Article 7 GDPR and by extension Article 17 (1) (b) GDPR.

ii. Interface-based patterns

Skipping – Deceptive snugness (Annex I checklist 4.2.1)

Example 56: In the process of deleting their account, users are provided with two options to choose from: To delete their account or to pause it. By default, the pausing option is selected.

177. The first option of deleting the account results in the deletion of all personal data of users, meaning that the social media platform is no longer in possession of these data, except for data under the temporary exception of Article 17 (3) GDPR. In contrast, with the second option of pausing the account, all personal data are kept and potentially processed by the social media provider. This necessarily poses more risks to the data subject, for example if a data breach happens and data still stored by the social media provider are accessed, duplicated, transferred or otherwise processed. The default selection of the pause option is likely to nudge users to select it instead of deleting their account as initially intended. Therefore, the practice described in this example can be considered as an infringement of Article 12 (2) GDPR since it does not, in this case, facilitate the exercise of the right to erasure, and even tries to nudge users away from exercising it.

Skipping – Look over there (Annex I checklist 4.2.2)

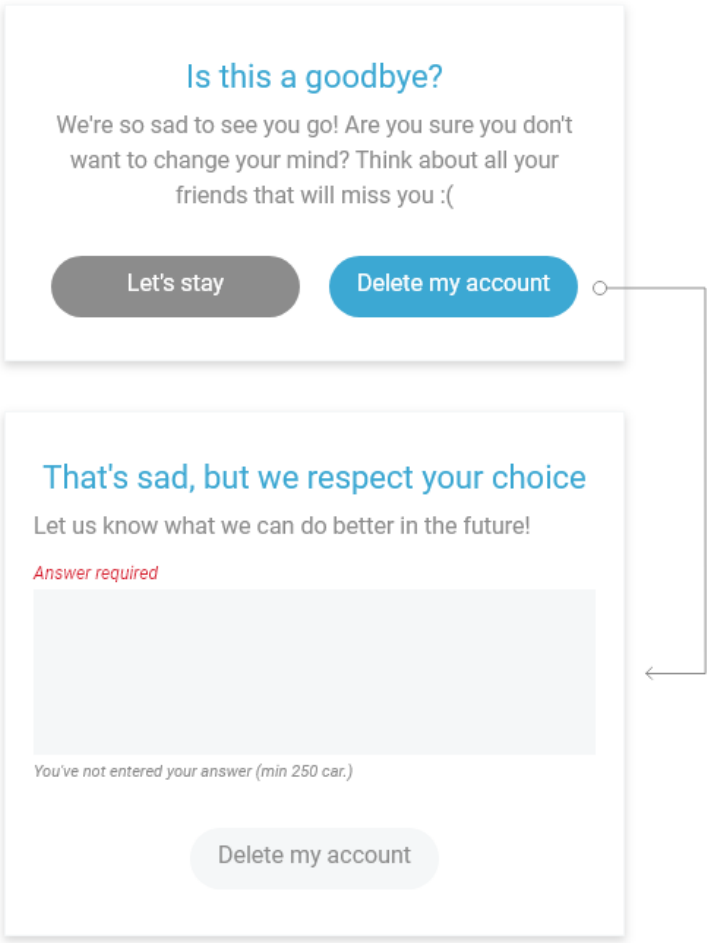
178. Providing users with a mean to download their data when they indicate their will to delete their account can be a relevant option to offer. Indeed, once their account is deleted, their personal data will be erased after a certain period of time. This means that, if they do not get a copy of their personal data, they will entirely lose them. However, the presentation of this option can constitute a ***Look over there*** deceptive design pattern, as shown in the following example.

Example 57: After clicking on "Delete my account", users are presented with the option to download their data, implemented as the right to portability, before deleting the account. When clicking to download their information, users are redirected on a download information page. However, once users have chosen what and how to download their data, they are not redirected to the deletion process.

179. In the example above, it could be considered that the way the download option is implemented does not facilitate the exercise of the right to erasure associated with the account's deletion. Indeed, once users have downloaded their data, they are not brought back to the deletion process. To go back to it, they will have to click several times. Hindering in such a way the exercise of a right infringes Article 12 (2) GDPR. Furthermore, providing a mean to easily reach the deletion process after downloading one's data is a simple feature to implement. In that regard, it could be considered that the obligation to implement appropriate technical and organisational measures in Article 25 (1) GDPR is not respected as users are not able to continue to exercise their rights effectively.

Obstructing – Longer than necessary (Annex I checklist 4.4.2)

180. As detailed in use case 4, any irrelevant steps added to the exercise of a right might contravene provisions of the GDPR, in particular Article 12 (2). This applies to the moment where users aim to delete their account, as it would interfere with the right to erasure associated with such a request.



Example 58: In this example, users first see a confirmation box to erase their account after having clicked on the corresponding link or button in their account. Even though there is some ***Emotional Steering*** in this box, this step can be seen as a security measure in order for users not to delete their account following a mis-click in their account. However, when users click on the "Delete my account" button, they are confronted with a second box asking them

to textually describe the reason they want to leave the account. As long as they have not entered something in the box, they cannot delete their account as the button associated with the action is inactive and greyed out. This practice makes the erasure of an account ***Longer than Necessary***, especially as asking users to produce a text describing why they want to leave an account requires extra effort and time and should not be mandatory to delete one's account.

181. As noted previously, when exercising a right, users should not have to answer questions not related to the exercise of the right itself. Having to justify one's choice or explain how the social media platform should improve does not fall under that category. In the illustrated example, this issue is heightened as data subjects have to write an answer instead of selecting a pre-made proposition in a list, which is even more burdensome for them since it requires to fully create the answer. Such mechanism could exclude some users from exercising their right altogether if they are not comfortable enough to write down an answer.

182. However, this does not mean that a list of pre-made answers is an acceptable step to add to the process of deleting one's account. This is especially true if these answers are associated with further steps and actions imposed on users, as the example below shows**.**

Example 59: The social media provider makes it mandatory for users to answer a question about their reasons for wishing to erase their account, through a selection of answers from a drop-down menu. It appears to users that answering this question (apparently) enables them to achieve the action they want, i.e. to delete the account. Once an answer is selected, a pop-up window appears, showing users a way of solving the issue stated in their answer. The question-answer process therefore slows down users in their account erasure process.

183. In addition to making the erasure of the account particularly lengthy, a ***Look Over There*** mechanism aims to divert users away from deleting their account by providing a solution to their motivation behind leaving the social media platform. These hinder the exercise of the right to erasure and, by extension, discourage the data subjects to exercise their right.

Fickle – Decontextualising (Annex I checklist 4.5.2)

184. Finally, the ***Decontextualising*** deceptive design pattern can also be found when users wish to delete their account.

Example 60: On the social media platform XY, the link to deactivate or delete the account is found in the "*Your XY Data*" tab.

185. In general, the terms used to title a page or section of the social media platform dedicated to data protection matters should clearly reflect the kind of information or control included there. Average users are unlikely to link actions to delete or deactivate their account to data management. In the previous example, users would not expect the functionality for deleting their account in a page called "Your XY Information" that alludes to seeing and potentially reviewing one's information. Instead, they would look for a "General" page or a "Delete my account" page. Therefore, from the view point of users, the options are placed in a setting that it is out of context and does not match user expectations.

Example 61: The actual tab to erase an account is found in the section "*delete a function of your account*".

186. In this example, users could mistakenly understand the section title as the mere place where to adjust single functions. Users would therefore not expect the option to delete the whole account to be there. That makes it hard for users to find the correct link to erase the entire account.

187. The ***Decontextualising*** deceptive design pattern, as illustrated in the two examples above, could be considered a breach of Article 12 (2) GDPR, given that users would have difficulties to find the right place where to exercise their right to erasure.

c. Best Practices

Coherent wordings: see use case 1 for definition (p.22).

Providing definitions: see use case 1 for definition (p.22).

Use of examples: see use case 1 for definition (p.22).

Explaining Consequences: see use case 2c for definition (p.32)**.**

Cross-device consistency: see use case 3a for definition (p.39)**.**

For the European Data Protection Board

The Chair

(Andrea Jelinek)

4 ANNEX I: LIST OF DECEPTIVE DESIGN PATTERN CATEGORIES AND TYPES

The following list provides an overview of deceptive design pattern categories and the types of deceptive design patterns within each category. It also lists the GDPR provisions most concerned by the deceptive design pattern types. Readers should keep in mind that, as mentioned above, the principle of fair processing laid down in Article 5 (1) (a) GDPR is a starting point for an assessment of existence of deceptive design patterns. It has an umbrella function and all deceptive design patterns would not comply with it irrespectively of compliance with other data protection principles.[81]

For each pattern, the list also contains the numbers of examples and corresponding use case (UC) to help readers find them quickly.

It is important to note that this list is not exhaustive and that deceptive design patterns can therefore also occur in use cases that do not contain an example for this deceptive design pattern type in the text of the Guidelines.

4.1 Overloading

Burying users under mass of requests, information, options or possibilities in order to deter them from going further and make them keep or accept certain data practice.

4.1.1 Continuous prompting[82]

Pushing users to provide more personal data than necessary for the purpose of processing or to agree with another use of their data by repeatedly asking users to provide data or to consent to a new purpose of processing. Such repetitive prompts can happen through one or several devices. Users are likely to end up giving in, wearied from having to refuse the request each time they use the platform which disrupts them in their use.

Concerned GDPR provisions:

- *Purpose limitation: Article 5 (1) (b);*
- *Freely given consent: Article 7* in conjunction with Article 4 (11);
- *Specific consent: Article 7 (2).*

Examples: UC 1 examples 1, 2; UC 3a example 34 (illustration).

4.1.2 Privacy Maze

When users wish to obtain certain information or use a specific control or exercise a data subject right, it is particularly difficult for them to find it as they have to navigate through too many pages in order to obtain the relevant information or control, without having a comprehensive and exhaustive overview available. Users are likely to give up or miss the relevant information or control.

Concerned GDPR provisions:

[81] See above, para. 9 of these Guidelines.
[82] This pattern is closely related to a type of pattern called "Nagging' found in the academic literature.

- *Principle of transparency*: *Article 5 (1) (a) and transparent information: Article 12 (1);*
- *Principle of fairness: Article 5 (1) (a);*
- *Easily accessible information*: Article 12 (1);
- *Easy access to rights*: Article 12 (2);
- *Informed consent*: Article 7 in conjunction with Article 4 (11).

Examples: UC 2a example 17; UC 3a example 33; UC 3b example 37; UC 4 examples 47 (illustration) and 48 (illustration); UC 5 example 51.

4.1.3 Too many options

Providing users with (too) many options to choose from. The amount of choices leaves users unable to make any choice or make them overlook some settings, especially if information is not available. It can lead them to finally give up or miss the settings of their data protection preferences or rights.

Concerned GDPR provisions:

- *Principles of transparency and fairness:* Article 5 (1) a;
- *Transparent information*: Article 12 (1).

Example: UC 3b example 35.

4.2 Skipping

Designing the interface or user journey in such a way that users forget or do not think about all or some of the data protection aspects.

4.2.1 Deceptive snugness

By default, the most data invasive features and options are enabled. Relying on the default effect which nudges individuals to keep a pre-selected option, users are unlikely to change this even if given the possibility.

Concerned GDPR provisions:

- *Data protection by design and by default*: Article 25 (1);
- *Consent:* Articles 4 (11) and 6 (illegal practice to activate a processing based on consent by default).

Examples: UC 1 example 9; UC 3b examples 39 and 40 (illustration); UC 5 example 55.

4.2.2 Look over there

A data protection related action or information is put in competition with another element which can either be related to data protection or not. When users choose this distracting option, they are likely to forget about the other, even if it was their primary intent.

Concerned GDPR provisions:

- *Principles of transparency and fairness:* Article 5 (1) a;
- *Transparent information*: Article 12 (1);
- *Exercise of rights:* Article 12 (2).

Examples: UC 2c example 25; UC 3a example 29; UC 5 examples 56 and 58.

4.3 Stirring

Affecting the choice users would make by appealing to their emotions or using visual nudges.

4.3.1 Emotional Steering[83]

Using wording or visual elements (such as style, colours, pictures or others) in a way that confers the information to users in either a highly positive outlook, making users feel good, safe or rewarded, or in a highly negative one, making users feel scared, guilty or punished. Influencing the emotional state of users in such a way is likely to lead them to make an action that works against their data protection interests.

Concerned GDPR provisions:

- *Principles of transparency and fairness:* Article 5 (1) a;
- *Transparent information*: Article 12 (1);
- *Exercise of rights:* Article12 (2)*;*
- *Child's consent:* Article 8;
- *Informed consent*: Article 7 in conjunction with Article 4 (11);

Examples: UC1 examples 4, 5, 6; UC 5 example 52.

4.3.2 Hidden in plain sight

Use a visual style or technique for information or data protection controls that nudges users toward less restrictive and thus more invasive options.

Concerned GDPR provisions:

- *Principle of fairness*: Article 5 (1) a;
- *Freely given consent:* Article 7 in conjunction with Article 4(11);
- *Clear information*: Article 12 (1);
- *Exercise of rights:* Article12 (2)

Examples: UC1 example 8, UC 3a example 34 (illustration); UC 3b example 40 (illustration); UC 4 example 48.

[83] This pattern is closely related to a type of pattern called "*Toying with Emotions*" found, inter alia, in reports of intergovernmental organisations such as European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., et al., *Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation : final report*, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2838/859030 and OECD (2022), "Dark commercial patterns", *Documents de travail de l'OCDE sur l'économie numérique*, n° 336, Éditions OCDE, Paris, https://doi.org/10.1787/44f5e846-en.

4.4 Obstructing[84]

Hindering or blocking users in their process of obtaining information or managing their data by making the action hard or impossible to achieve.

4.4.1 Dead end

While users are looking for information or a control, they end up not finding it as a redirection link is either not working or not available at all. Users are left unable to achieve that task.

Concerned GDPR provisions:

- *Easily accessible information*: Article 12 (1);
- *Exercise of rights*: Article 12 (2);
- *Data protection by design and by default*: Article 25 (1).

Examples: UC1 examples 10, 11; UC 2a example 18; UC 3a examples 30, 31; UC 4 example 43.

4.4.2 Longer than necessary

When users try to activate a control related to data protection, the user journey is made in a way that requires more steps from users, than the number of steps necessary for the activation of data invasive options. This is likely to discourage them from activating such control.

Concerned GDPR provisions:

- *Easily accessible information*: Article 12 (1);
- *Exercise of rights*: Article 12 (2);
- *Right to object*: Article 21 (1);
- *Consent withdrawal*: Article 7 (3);
- *Data protection by design (and by default)*: Article 25 (1).

Examples: UC 1 example 7; UC 3a example 32; UC 4 example 50; UC 5 examples 57 (illustration) and 58.

4.4.3 Misleading action

A discrepancy between information and actions available to users nudges them to do something they do not intend to. The difference between what users expect and what they get is likely to discourage them from going further.

Concerned GDPR provisions:

- *Transparent information*: Article 12 (1);
- *Fairness of processing*: Article 5 (1) (a).

[84] This category is closely related to the strategy called *"Obstruction"* defined and described in Gray Colin M., Kou Yubo, Battles Bryan, Hoggatt Joseph, and Toombs Austin L. 2018. The Dark (Patterns) Side of UX Design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (Montreal QC, Canada) (CHI '18). ACM, New York, NY, USA, Article 534, 14 pages. https://doi.org/10.1145/3173574.3174108.

- *Informed consent*: Article 7 (2) in conjunction with Article 4 (11).

Examples: UC 1 example 3; UC 3a example 28.

4.5 Fickle

The design of the interface is unstable and inconsistent, making it hard for users to figure out the nature of the processing, to properly make a choice concerning their data, and to find where the different controls are.

4.5.1 Lacking hierarchy

Information related to data protection lacks hierarchy, making information appear several times and being presented in several ways. Users are likely to be confused by this redundancy and to be left unable to fully understand how their data are processed and how to exercise control over them.

Concerned GDPR provisions:

- *Easily accessible information*: Article 12 (1);
- *Exercise of the rights: Article 12 (2).*

Examples: UC 2a examples 13 and 14.

4.5.2 Decontextualising

A data protection information or control is located on a page that is out of context. Users are unlikely to find the information or control as it would not be intuitive to look for it on this specific page.

Concerned GDPR provisions:

- *Easily accessible information*: Article 12 (1);
- *Transparent information*: Article 12 (1);
- *Exercise of the rights: Article 12 (2).*

Examples: UC 3b examples 41, 42; UC 5 examples 59 and 60.

4.5.3 Inconsistent interface

An interface is not consistent across different contexts (e.g., a data protection related menu does not display the same items on mobile and on desktop) or with users' expectations (e.g., an option whose location has been switched with that of another option). These differences can lead users not to find the desired control or information or to interact with an element of the interface out of habits even though this interaction leads to make a data protection choice users do not want.

Concerned GDPR provisions:

- *Easily accessible information*: Article 12 (1);

- *Exercise of the rights: Article 12 (2).*

Examples: UC 3b example 39; UC 4 example 50.

4.5.4 Language discontinuity

Information related to data protection is not provided in the official language(s) of the country where users live, whereas the service is. If users do not master the language in which data protection information is given, they will not be able to easily read it and therefore likely to not be aware of how data are processed.

Concerned GDPR provisions:

- *Fairness of processing*: Article 5 (1) (a);
- *Intelligible information*: Article 12 (1), Article 13 and Article 14;
- *Use of clear and plain language for the information*: Article 12 (1), Article 13 and Article 14.

Examples: UC 2a example 16; UC 3a examples 26 (illustration) and 27; UC 4 example 44.

4.6 Left in the dark

The interface is designed in a way to hide information or controls related to data protection or to leave users unsure of how data is processed and what kind of controls they might have over it.

4.6.1 Conflicting information

Giving pieces of information to users that conflict with each other in some way. Users are likely to be left unsure of what they should do and about the consequences of their actions, therefore likely not to take any and to just keep the default settings.

Concerned GDPR provisions:

- *Fairness of processing*: Article 5 (1) (a);
- *Transparent information*: Article 12 (1);
- *Informed consent*: Article 7 (2) in conjunction with Article 4 (11).

Examples: UC 2a example 12; UC 2c example 20; UC 3b example 36.

4.6.2 Ambiguous wording or information

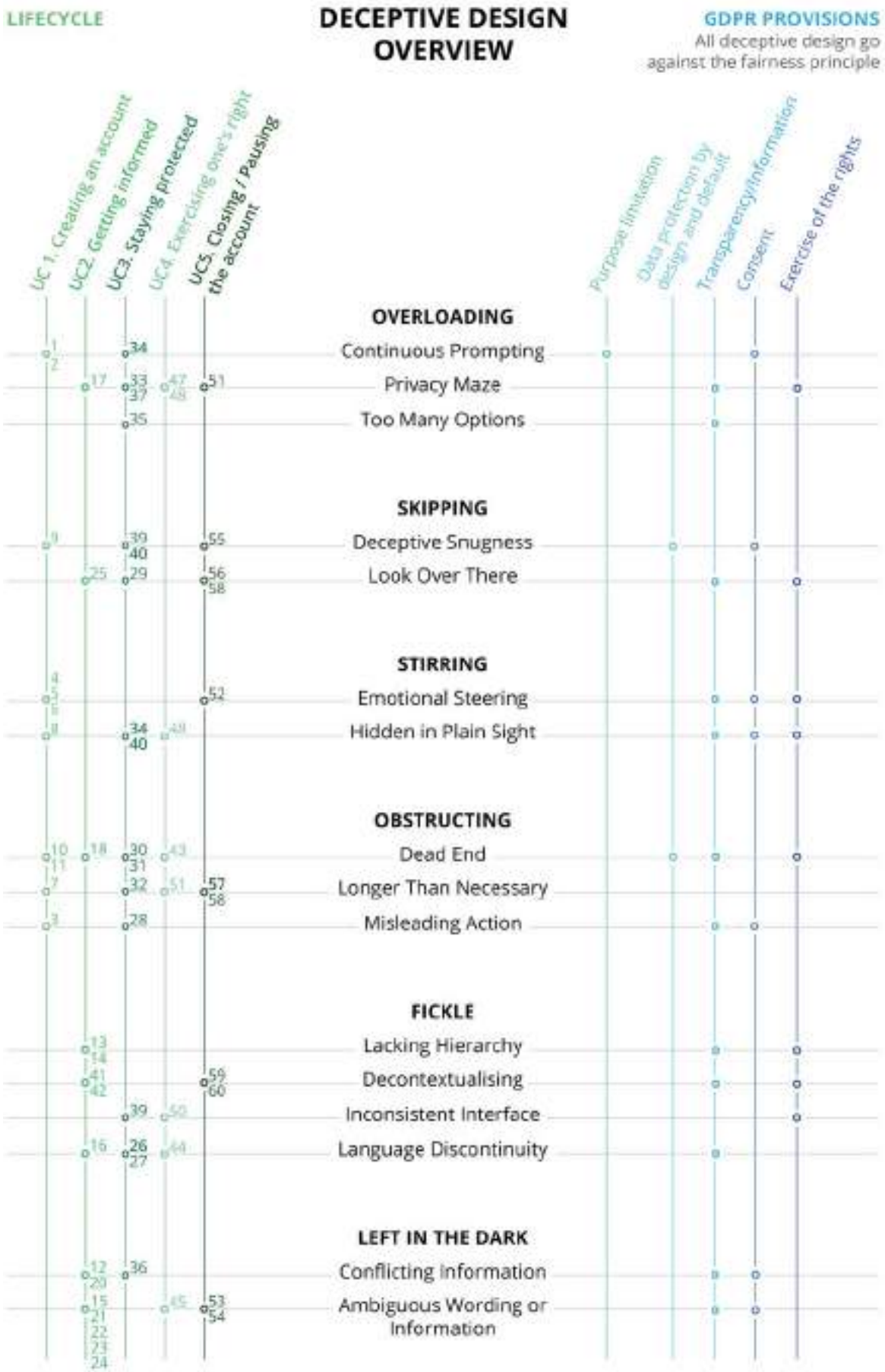
Using ambiguous and vague terms when giving information to users. They are likely to be left unsure of how data will be processed or how to exercise control over their personal data.

Concerned GDPR provisions:

- *Fairness of processing*: Article 5 (1) (a);
- *Transparent information*: Article 12 (1);
- *Use of clear and plain language for the information*: Article 12 (1);

- *Informed consent*: Article 7 (2) in conjunction with Article 4 (11);
- *Incomplete information*: Article 13
- *Specific provisions depending on the particular use case, for example* Article 34 *for UC 2c*.

Examples: UC 2a example 15; UC 2c examples 21, 22, 23, 24; UC 4 example 45; UC 5 examples 53 and 54.


LIFECYCLE
DECEPTIVE DESIGN OVERVIEW
GDPR PROVISIONS
All deceptive design go against the fairness principle
UC 1. Creating an account
UC2. Getting informed
UC3. Staying protected
UC4. Exercising one's right
UC5. Closing / Pausing the account
Purpose limitation
Data protection by design and default
Transparency/information
Consent
Exercise of the rights
OVERLOADING
Continuous Prompting
Privacy Maze
Too Many Options
SKIPPING
Deceptive Snugness
Look Over There
STIRRING
Emotional Steering
Hidden in Plain Sight
OBSTRUCTING
Dead End
Longer Than Necessary
Misleading Action
FICKLE
Lacking Hierarchy
Decontextualising
Inconsistent Interface
Language Discontinuity
LEFT IN THE DARK
Conflicting Information
Ambiguous Wording or Information

5 ANNEX II: BEST PRACTICES

The following list provides an overview of best practices described in the Guidelines at the end of each use case. These can be used to design user interfaces which facilitate the effective implementation of the GDPR. Such best practices can offer a first step toward a standardised way for users to effectively control their data and exercise their rights.

Shortcuts: Links to information, actions or settings that can be of practical help to users to manage their data and their data protection settings should be available wherever they are confronted to related information or experience (*e.g. links redirecting to the relevant parts of the privacy policy*; *e.g. in the privacy policy, provide for each data protection information links that directly redirects to the related data protection pages on the social media platform; provide users with a link to reset their password*; *when users are informed about an aspect of the processing, they are invited to set their related data preferences on the corresponding setting/dashboard page; provide a link to account deletion in the user account*)**.**

Bulk options: Putting options that have the same processing purpose together, so that users can change them more easily, while still leaving users the possibility to make more granular changes. If social media platforms present bulk options, these should not contain unexpected or unrelated elements (for example elements with different purposes). If the processing require consent, the bulk options must be in line with the EDPB Guidelines on consent, especially para. 42-44.

Contact information: The company contact address for addressing data protection requests should be clearly stated in the privacy policy. It should be present in a section where users can expect to find it, such as a section on the identity of the data controller, a rights related section or a contact section.

Reaching the supervisory authority: Stating the specific identity of the supervisory authority and including a link to its website or the specific website page related to lodging a complaint. This information should be present in a section where users can expect to find it, such as a rights related section.

Privacy Policy Overview: At the start / top of the privacy policy, include a (collapsible) table of contents with headings and sub-headings that shows the different passages the privacy notice contains. The names of the single passages clearly lead users regarding the exact content and allow them to quickly identify and jump to the section they are looking for.

Change spotting and comparison: When changes are made to the privacy notice, make previous versions accessible with date of release and highlight changes.

Coherent wordings: Across the website, the same wording and definition is used for the same data protection. The wording used in the privacy policy should match the one used on the rest of the platform.

Providing definitions: When using unfamiliar or technical words or jargon, providing a definition in plain language will help users understand the information provided to them. The definition can be given directly into the text, when users hover over the word, as well as be made available in a glossary.

Contrasting Data protection elements: Making data protection related elements or actions visually striking in an interface that is not directly dedicated to the matter. For example, when posting a public

message on the platform, controls over association of the geolocation should be directly available and clearly visible.

Data Protection Onboarding: Just after the creation of an account, include data protection points within the onboarding experience of the social media provider for users to smoothly discover and set their preferences. For example, this can be done by inviting them to set their data protection preferences after adding their first friend or sharing their first post.

Use of examples: In addition to mandatory information clearly and precisely stating the purpose of processing, examples can be used to illustrate a specific data processing to make it more tangible for users.

Sticky navigation: While consulting a page related to data protection, the table of contents can be constantly displayed on the screen allowing users to always situate themselves on the page and to quickly navigate in the content thanks to anchor links.

Back to top: Include a return to top button at the bottom of the page or as a sticky element at the bottom of the window to facilitate users' navigation on a page.

Notifications: Notifications can be used to raise awareness of users on aspects, change or risks related to personal data processing (*e.g. when a data breach occurred*). These notifications can be implemented in several ways, such as through inbox messages, pop-in windows, fixed banners at the top of the webpage, etc.

Explaining consequences: When users want to activate or deactivate a data protection control, or give or withdraw their consent, inform them in a neutral way on the consequences of such action.

Cross-device consistency: When the social media platform is available through different devices (e.g. computer, smartphones, etc.), settings and information related to data protection should be located in the same spaces across the different versions and should be accessible through the same journey and interface elements (menu, icons, etc.).

Data protection directory: For easy orientation through the different section of the menu, provide users with an easily accessible page from where all data protection related actions and information are accessible. This page could be found in the social media provider main navigation menu, the user account, through the privacy policy, etc.

Contextual information: in addition to an exhaustive privacy policy, bring short bits of information at the most appropriate time for the user to have a specific and continuous information on how their data are processed.

Self-explanatory URL: pages related to data protection settings or information should use a web address that clearly reflects their content. For example, a page centralising data protection control could have a URL such as [social-network.com]/data-settings.

Exercise of the rights form: to facilitate users in exercising their GDPR rights, provide a dedicated form that helps users understand their rights and that guides them carry out these kind of requests.