Feedback to the
Guidelines 3/2022 onDark patterns in social media platform interfaces: How to recognise and avoid them
Version 1.0, Adopted on 14 March 2022

Students of the Master Course Law and Technology in Europe,
Utrecht University[1]

1. Scope

> 3. In the context of these Guidelines, "DPs" are considered interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions in regards of their personal data. (…)

Anti-patterns. According to Greenberg et al.[2], "*sometimes deception occurs unintentionally. Due to a lack of technical skills, inexperience or little knowledge of user needs, a designer can design a non-working solution that results in an* ***unintended negative user experience****".*Such a design solution is often called an *anti-pattern*. When an anti-pattern is discovered, it is often documented as 'known bad practice', so the use of the design solution can be prevented in future UI design."[3] We believe that the **intent is not needed to prove/provide evidence thereof**, but what matters is the impact of the design of DPs upon users.[4] However, it may be **useful to differentiate between anti-pattern and DPs** within the guidelines and to elaborate whether intent would be taken into consideration. **(Magdalena and Elena)**

> 4. DPs do not necessarily only lead to a violation of data protection regulations. DPs can, for example, also violate consumer protection regulations. The boundaries between infringements enforceable by data protection authorities and those enforceable by national consumer protection authorities can overlap.

Enforcement of the GDPR. The 2019 Guidelines on Art. 25 GDPR by design and by default already referred that *options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design*.[5] Those Guidelines, however, have not been sufficient to reduce DPS by social media interfaces designers.

Enforcement of DPs provisions seems to be harder than other areas especially because infringements can relate to different regulations. It could be this part which lacks clarity what makes DPs a commonly used practice.[6] However, it is clear by the following lines that DPs, even being undesirable, may not always be unlawful. If these guidelines are indeed aiming for increasing the lawfulness of social media interface design regarding DPs, then it would be recommendable to also clarify the enforcement and consequences of using DPs. **(Solène Tobler + Isabel Sierra Rubio)**

> 7. It is essential to keep in mind that dark patterns raise additional concerns regarding potential impact on children, registering with the social media provider. (…)

[1] 1 Law and Technology in Europe, https://www.uu.nl/masters/en/law-and-technology-europe

[2] Saul Greenberg, Sebastian Boring, Jo Vermeulen, and Jakub Dostal. 2014. Dark patterns in proxemic interactions: a critical perspective. In Proceedings of the 2014 conference on Designing interactive systems. ACM, 523–532

[3] Kristi Bergman, 'DPs: Malicious Interface Design from a User's Perspective' (Master thesis, University of Utrecht 2021)

[4] https://points.datasociety.net/dark-patterns-and-design-policy-75d1a71fbda5

[5] 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.

[6] The European Consumer Organisation. (2022). "DPs" and the EU consumer law acquis. Recommendations for better enforcement and reform. [Review of "DPs" and the EU consumer law acquis. Recommendations for better enforcement and reform.]. Available at https://www.beuc.eu/publications/beuc-x-2022-013_dark_patters_paper.pdf.

- **Vulnerable users** need to be provided an easier understandable explanation of context and agreement when signing up. Vulnerable users mentioned here are not limited to children, because **layers of vulnerability** are not fixed attributes of specific individuals or groups but are features constructed by **status, time, and location**.[7] For example, people in different social contexts (like education level) will have different abilities to identify DPs. From the research, education levels above the high-school degree positively correlate with identifying the DPs.[8] Thus, controllers should first determine the layers of vulnerability of users when using their website. If such communication is addressed to persons with reduced understanding, data controllers might be required to give information in a way that needs to be easily understandable by every recipient.[9] **(Dina Kristina Denso+Shuoyuan Jiang)**

Children. According to the updated "*Meta Platforms Ireland Limited*" Terms of Use,[10] -including *Instagram from Meta*- are part of the registration process. The user must assure that she is over **thirteen (13) years old.**[11] Recital 38 GDPR says that **children** deserve special protection regarding their personal data since they may be less aware of the risks, implications, and safeguards of processing personal data.The GDPR explicitly recognises children as a vulnerable group of data subjects.[12]
Considering that privacy notices and Terms of Use are usually long texts with legal terms that a child cannot efficiently follow, the data controller must explain to them how she uses their personal data.
For example, in the beginning of the sign-up process a **short video presentation or the use of images (pictorial versions[13])** next to small texts summarising the important points of Privacy Policy and the Terms of Use of a website could be more effective to them. In this way, children are more responsive to information provided visually than long academically written texts.[14] Specifically, visual instructions are 323% more likely to be followed by children than text-only instructions.[15]According to the ICO, if the data controller decides to provide only one version of the Privacy Notice, she must ensure that it is comprehensible to all different ages, even to the youngest audience.[16] (**Evangelia Cheiladaki + Eleni Arampatzi**)

9. 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 DPs could infringe those provisions.

Measurable thresholds. The Guidelines mention data protection principles and Article 25 as the basis for the assessment of the existence of DPs without providing a **measurable threshold** for identifying a DPs.

[7] Gianclaudio Malgieri and Jędrzej Niklas, 'Vulnerable data subjects', Computer Law & Security Review,Volume 37,2020

[8] Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig, and Gabriele Lenzini. 2021. "I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!" - DPs from the End-User Perspective. In Designing Interactive Systems Conference 2021 (DIS '21). Association for Computing Machinery, New York, NY, USA, 763–776.

[9] Gianclaudio Malgieri and Jędrzej Niklas, 'Vulnerable data subjects', Computer Law & Security Review,Volume 37,2020

[10] Instragram Help Center. (2022, March 31). *Terms of Use*. Retrieved March ,31, 2022, from https://help.instagram.com/581066165581870

[11] Schneble, C., O., Favaretto, M., Elger, S., B., Shaw, D., M. (2021). Social Media Terms and Conditions and Informed Consent From Children: Ethical Analysis. *JMIR Pediatr Parent 2021;4(2):e22281*. doi: 10.2196/22281

[12] Milkaite, I. , Lievens, E. Children's Rights to Privacy and Data Protecton Aroundthe World: Challenges in the Digital Realm. (2019). *European Journal of Law and Technology, 10 (1).*

[13] *Schneble, C., O., Favaretto, M., Elger, S., B., Shaw, D.*, M. (2021). Social Media Terms and Conditions and Informed Consent From Children: Ethical Analysis. *JMIR Pediatr Parent 2021;4(2):e22281*. doi: 10.2196/22281

[14] Welsch, C. (2021, May 26). *Learning through looking*. Retrieved April, 12, 2022, from https://www.eib.org/en/stories/learn-with-images.

[15] Bilyana Nikolaeva (2017). *Visuals for Kids: Enhancing Communication and Learning*. Retrieved April, 12, 2022, from https://graphicmama.com/blog/visuals-kids-learning-education/

[16] Information Commission's Office. (2020, 21 October). *Right of access*. Retrieved March, 31, 2022, from https://ico.org.uk/for-organisations/guide-to-dataprotection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/?template=pdf&patch=19#link8

Although the Guidelines mention in Parag 11 research methods that can be used to demonstrate compliance with the GDPR, it is not defined what metrics would suggest the existence of a DPs when, for instance, using A/B testing. Neither is this clarified in Guidelines 4/2019 on Article 25, which mention possible KPIs controllers could use to demonstrate effective implementation of data protection principles, however, leave their determination to controllers.[17]

Thus, to assist social media providers when drawing the line between permissible persuasion and DPs that violate users' autonomy,[18] the Guidelines should consider introducing a measurable threshold.

The Guidelines could take into account the threshold proposed by *Luguri and Strahilevitz* – an *over doubled acceptance rate in comparison to an alternative user interface* – as their research showed a considerably higher acceptance rate in connection to pop-ups where there was a DPs present.[19] Accordingly, social media providers could use A/B testing to compare two user interfaces (specifically: pop-ups) and based on the acceptance rate, establish whether one contains DPs.

Alternatively, a DPs could be established on the basis of a user study showing that a *significant minority of users* have been *misled* by an element of the user interface into making an unintended decision in regards of their personal data, which would not require a comparison between two user interfaces.[20] (**Eva Opsenica + Joanna Taneva**)

17. Compliance with Data Protection by Default and Data Protection by Design is important when assessing DPs, as it would result in avoiding implementing them in the first place.

Power balance and certification schemes. The Guidelines list **power balance** as one of the DPbDD elements social media providers must consider when implementing data protection by design[21] to avoid the implementation of DPs. According to the Guidelines 4/2019, power imbalances should be avoided, and where this is not possible, accounted for with suitable measures. Yet, in the online ecosystem, power imbalances between users and dominant platforms are unavoidable.[22] As social media platforms are in control of the choice architecture of the service and access to data, have greater bargaining power, and possess detailed knowledge on users' characteristics,[23] users' choice in the sense of individual autonomy, self-determination, and privacy becomes disrupted.[24] Therefore, power imbalances should be mitigated with **measures** safeguarding and empowering users – beyond merely providing them with more information.[25]

- The EDPB should consider measures recommended by **BEUC:** that consumer protection bodies carry out "sweep" investigations on the use of DPs, test user interfaces, and provide guidance to companies on the design of their choice architecture.[26] The EDPB could be inspired by these same recommendations.

-The EDPB could encourage DPAs to create a **certification mechanism** (Article 58(3)) pursuant to Article 42 to demonstrate compliance with Article 25 – specifically in connection to the design of user interfaces. A certification mechanism could incentivise controllers to earn the certification and comply with DPA's

[17] EDPB Guidelines 4/20219 on Article 25 Data Protection by Design and by Default, para. 16.

[18] Mathur, A., Kshirsagar, M., & Mayer, J. (2021, May). What Makes a Dark Pattern. . . Dark? *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, p. 19. https://doi.org/10.1145/3411764.3445610

[19] Luguri, J., & and Strahilevitz, L. J. (2021). Shining a light on DPs. *Journal of Legal Analysis, 13(1)*, 43-109. https://doi.org/10.1093/jla/laaa006

[20] Federal Trade Commission. *The FTC's Endorsement Guides: What People Are Asking*. https://www.ftc.gov/business-guidance/resources/ftcs-endorsement-guides-what-people-are-asking

[21] EDPB Guidelines 4/20219 on Article 25 Data Protection by Design and by Default, para 16.

[22] The European Consumer Organisation. (2022). *EU consumer protection 2.0 – Protecting fairness and consumer choice in a digital economy*, p. 2. https://www.beuc.eu/publications/eu-consumer-protection-20-protecting-fairness-and-consumer-choice-digital-economy/html; para. 21.

[23] Ibidem, para. 10.

[24] Ibidem para. 17.

[25] Ibidem para. 13.

[26] The European Consumer Organisation. (2022). *"DPs" and the EU consumer law acquis*, p. 12. https://www.beuc.eu/publications/dark-patterns-and-eu-consumer-law-acquis/html

requirements.[27] As a certification mechanism would require the DPA to periodically review (Article 57(1)(o)) and possibly withdraw certifications (Articles 58(2)(h)), controllers would be nudged to improve their user interfaces to users' benefit.[28] In this regard, a certification mechanism would also specify the latest technological advances that controllers must take into account, thereby assisting them with complying with Article 25.[29] Lastly, a certification mechanism could empower users by allowing them to quickly assess whether a user interface is 'safe' (recital 100). (**Eva Opsenica + Joanna Taneva**)

The EDPB could implement provisions that would facilitate the work of programmers and developers of social media platform interfaces. For instance, the ACM Code of Ethics encourages computing professionals to be "*honest and trustworthy*" and "*ensure that the public good is the central concern*", therefore a uniform way would create a positive influence on their practice.[30] Another example emphasizing a good practice is the study conducted among participants of the business development program for the entrepreneurs which concluded that some practices cannot be pursed: i) lying to the customer, ii) applying a countdown timer; iii) informing customers that the product is running out of stock.[31]Another possibility is the use of AI. Some studies argue that *'automated techniques can discover and identify DPs by simulating user actions and analyzing the dataset and the text'*.[32] Furthermore, the utilization of static analysis tools can also contribute to the process of elimination of DPs.[33] (**Dušan Stevanović**)

2. Opening a social media account

19. 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 don't read privacy policies. The most common problems relating to the understandability of privacy policies are its accessibility, readability, time consuming for users to read and lack of user motivation to read the policy.[34] Users will not read all the privacy policies they encounter prior to signing up with a social media platform due to its length and low-readable nature. A study suggested that users spend on average 250+ hours a year just to read privacy policies.[35]

State of the art methods applied to privacy policies. The problem of 'informed' consent in this regard has been the subject of extensive research in various studies.[36] These studies have explored several avenues

[27] Reidenberg, J. R., Russell, N. C., Herta, V., Sierra-Rocafort, W., & Norton, T. B. (2019). Trustworthy Privacy Indicators: Grades, Labels, Certifications, and Dashboards. *Washington University Law Review, 96(5)*, 1409-1460, 1419. https://heinonline.org/HOL/LandingPage?handle=hein.journals/walq96&div=47&id=&page=

[28] Ibidem p. 1414.

[29] EDPB Guidelines 4/20219 on Article 25 Data Protection by Design and by Default, para. 19-22.

[30] Chris Brown and Chris Parnin, 'DPs for Influencing Developer Behavior' (2021) ACM <DPs for Influencing Developer Behavior (chbrown13.github.io)> accessed 17 April 2022

[31] Rikkard Harr and Annakarin Nyberg 'It depends upon whether it's true or not: Entrepreneurs Perspective on Dark Designed Patterns' (What Can CHI Do About DPs? CHI Workshop - May, 2021, Online Virtual Conference)

[32] Frode Guribye et al? DPs in cookie consent notices: new definitions and mitigation strategies. (What can CHI do about DPs? CHI Workshop - May, 2021,

[33] ibid.

[34] Schimidt, K (2018), 'Empowering users to understand their online privacy rights and choices through an interactive social media sign-up process', 3

[35] McDonald, A. M., & Cranor, L. F. (2008). *The Cost of Reading Privacy Policies.* A Journal of Law and Policy for the Information Society, 4(3), 543–568

[36] See also: Brustoloni, J. C., & Villamarín-Salomón, R. (2007). *Improving security decisions with polymorphic and audited dialogs.* Proceedings of the 3rd Symposium on Usable Privacy and Security - SOUPS '07, 76. https://doi.org/10.1145/1280680.1280691; Chee, F. M., Taylor, N. T., & de Castell, S. (2012) . *Re-Mediating Research Ethics.* Bulletin of Science, Technology & Society, 32(6), 497–506. https://doi.org/10.1177/0270467612469074; Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., ... Hall, S. (2005) *Stopping Spyware at the Gate: A User Study of Privacy,*

for increased information design, such as the provision of **summaries in layman's terms**, using **visuals such as clips or pictures**, and different information types to create **'textured agreements' which are visually redesigned agreements that employ visual design techniques such as typography and layout.**[37] To this end, social media platforms should adopt state of the art technologies by utilising textured agreements for increased information design as user studies have shown that user reading time was increased by 30 seconds in textured agreements when compared to plain-text privacy agreements. Therefore, Schmidt advocates for an ethical design by texturizing the privacy notice and terms of use, thereby promoting a truly interactive experience for the user, not just a click on 'agree'.[38] For example, a study conducted by Schmidt in 2018 found that by singling out the terms most worrying to users, thereby giving user a choice, writing for how users read on the web, and moving the information into the workflow of the sign-up process improved the user experience with policies.[39]

Mental models. Whilst aesthetic changes may make privacy policies more understandable, the fundamental problem of inaccurate mental models[40] of what policy agreements are and how the user should engage with it, is not addressed.[41] Even if individuals had sight of the complete privacy policy of the social media platform and the information contained therein, they would still be unable to process and act optimally on the overwhelming amounts of information– especially in the face of complex, ramified consequences associated with the protection or release of personal information.[42] This is supported by the theory of social media fatigue, which provides that too much information originating from social media platforms can lead to feelings of being overwhelmed.[43] Thus, the bounded rationality[44] inherent in humans limits their ability to acquire, memorise and process all relevant information, making them rely on simplified mental models, approximate strategies and heuristics.

User study. We therefore suggest that the EDPB conduct an updated user study to determine user attitudes, perceptions and misconceptions towards privacy policies for social media accounts by re-designing the sign-up process to encourage more interaction with the privacy policy terms. **(Jasper Hille + Roberto de Alcântara)**

Notice and Spyware Anti-Spyware Technology. Symposium On Usable Privacy and Security, 1–10. https://doi.org/10.1145/1073001.1073006; Good, N. S., Grossklags, J., Mulligan, D. K., & Konstan, J. a. (2007). *Noticing notice.* Proc. CHI '07, ACM Press, 607. https://doi.org/10.1145/1240624.1240720; Egelman, S., Tsai, J., Cranor, L., & Acquisti, A. (2009). *Timing is everything? The effects of timing and placement of online privacy indicators.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 319–328. https://doi.org/10.1145/1518701.1518752; Jensen, C., & Potts, C. (2004). *Privacy policies as decision-making tools.* Proceedings of the 2004 Conference on Human Factors in Computing Systems - CHI '04, 6(1), 471–478. https://doi.org/10.1145/985692.985752; Kay, M., & Terry, M. (2010). *Textured agreements: re-envisioning electronic consent.* SOUPS '10: Proceedings of the Sixth Symposium on Usable Privacy and Security, 1–13. https://doi.org/http://doi.acm.org/10.1145/1837110.1837127; McDonald, A. M., & Cranor, L. F. (2008). *The Cost of Reading Privacy Policies.* A Journal of Law and Policy for the Information Society, 4(3), 543–568; McKee, H. A. (2011). *Policy Matters Now and in the Future: Net Neutrality, Corporate Data Mining, and Government Surveillance. Computers and Composition,* 28(4), 276–291 https://doi.org/10.1016/j.compcom.2011.09.001; and The Center for Information Policy Leadership, 2013) The Center for Information Policy Leadership, H. & W. L. (2013). *Ten steps to develop a multilayered privacy notice.* Journal of Chemical Information and Modeling, 53(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004.

[37] Kay, M., & Terry, M. (2010). *Textured agreements: re-envisioning electronic consent.* SOUPS '10: Proceedings of the Sixth Symposium on Usable Privacy and Security, 1–13. https://doi.org/http://doi.acm.org/10.1145/1837110.1837127)

[38] Kiley Schmidt, 'Empowering users to understand their online privacy rights and choices through an interactive social media sign-up process.' (2018)

[39] Ibidem.

[40] Kiley Schmidt, 'Empowering users to understand their online privacy rights and choices through an interactive social media sign-up process.' (2018)

[41] ibidem

[42] Alessandro Acquisti and Jens Grossklags. 'Privacy and rationality in individual decision making.' *IEEE security & privacy* 3.1 (2005)

[43] Laura F. Bright, Susan Bardi Kleiser, and Stacy Landreth Grau. 'Too much Facebook? An exploratory examination of social media fatigue.' *Computers in Human Behavior* 44 (2015)

[44] Herbert A. Simon, 'Models of Bounded Rationality, vols. 1 and 2.' *Economic Analysis and Public Policy, MIT Press, Cambridge, Mass* (1982).

As a variety of data is being requested in the process of signing-up to create an account, the guidelines could introduce **attribute-dependent friction**[45] which could take the form of platforms being under an obligation to **colour code their different requests for personal data, depending on their sensitivity and potential implications for a user's privacy**.[46] As such, the user will be more likely to reflect upon the categories of data they are willing to share and deliberate on the consequences of sharing. *Jacobs et al*, in their discussion of the IRMA (a mobile application for identity management, enabling users to selectively share their information with different websites) acknowledge that **color-coding could enhance an individual's perception of sensitivity of the data that they would be agreeing on sharing and thus carefully considering their choice, in line with the concept of reflective design**.[47]

An approach to colour coding could be the adoption of universally recognized safety colours such as red, orange, yellow which are typically associated with danger, warning, and caution, respectively.[48] This could draw the attention of the user to potentially dangerous implications to their privacy, were they to consent to or grant that specific data, inviting them to reflect on the data which they are sharing. For example:

- as acknowledged by the guideline itself in paragraph 31 - requesting one's phone number is more intrusive data than one's e-mail.
- citizen identity numbers (e.g BSN in the Netherlands) are redundant when signing up for a platform, thus could be associated with red;
- categories of sensitive data, such as relating to political beliefs should also prompt a warning for the user to be able to reflect on the implications of sharing that data. This is especially relevant for users considering the revealed information following the Cambridge Analytica scandal and how social media platforms politically target their users.[49] **(Urszula Baranowska + Thalis Cabral)**

20. 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.

More consideration should be given to how **elderly people, people with cognitive disabilities and visually impaired persons** comprehend what they are signing up for.

The “easily accessible” requirement refers to the data subject’s option not to search for further information, but it should be instantly evident where this information can be found.[50] This applies to:

- people with motor, linguistic and cognitive disabilities – they interact more effectively with the help of **voice assistants'** use in their everyday life.[51]

[45] Terpstra, A., Schraffenberger, H., & Graßl, P. (2020). *Think before you click: how reflective patterns contribute to privacy* [Review of *Think before you click: how reflective patterns contribute to privacy*]. Radboud Repository. https://repository.ubn.ru.nl/bitstream/handle/2066/246490/246490.pdf?sequence=1&isAllowed=y

[46] Ibidem

[47] Jacobs, B., & Schraffenberger, H. (2020). Friction for Privacy: why privacy by design needs user experience design [Review of *Friction for Privacy: why privacy by design needs user experience design*]. *European Cyber Security Perspectives*, *7*, 11–14. https://www.overons.kpn/content/downloads/news/European-Cyber-Security-Perspectives-KPN-2020.pdf

[48] Braun, C. C., Mine, P. B., & Clayton Silver, N. (1995). The influence of color on warning label perceptions. International Journal of Industrial Ergonomics, 15(3), 179–187. https://doi.org/10.1016/0169-8141(94)00036-3

[49] Graham-Harrison, E., & Cadwalladr, C. (2018, March 17). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[50] Stanislaw Piasecki, Jiahong Chen. (2022). Complying with the GDPR when vulnerable people use smart devices. *International Data Privacy Law, 12.* https://doi.org/10.1093/idpl/ipac001

[51] Masina, F., Orso, V., Pluchino, P., Dainese, G., Volpato, S., Nelini, C., Mapelli, D., Spagnolli, A., & Gamberini, L. (2020). Investigating the Accessibility of Voice Assistants With Impaired Users: Mixed Methods Study. *Journal of medical Internet research*, *22*(9), e18431. https://doi.org/10.2196/18431

- older adults – these usually confront physical or health difficulties that make reading hard or challenging.[52] It should be clarified if it would be provided to them a pre-recorded short video or a voice assistance message presenting the data they sign up for. (**Evangelia Cheiladaki + Eleni Arampatzi**)

Di Geronimo et al. (2020)[53] conducted an online experiment in which participants were asked to rate the UI of several applications.[54] The experiment showed that most users did not recognise malicious designs (55%): 20% of users were unsure, and the remaining 25% were able to find the malicious designs in the apps presented. The study argues that because users are constantly being exposed to DPs, their attention is, arguably, fading. It also states that users may have developed a so-called "**DPs Blindness to malicious design**". Another user study found that that people under 40 and with higher education than high school diplomas are more likely to recognise DPs.[55]
Hence, we recommend the EDPB to consider providing means to mitigate the adverse effects that DPs practices have especially on **elderly people and people with a lower educational background (including children).** By creating this distinction, it would be possible to ensure a higher level of protection to the more vulnerable group. To eradicate DPs, we recommend to the EDPB to develop a non-exhaustive blacklist of forbidden practices which can be updated from time-to-time. (**Magdalena and Elena**)

Consumer law and data protection. When a user decides to sign-up to a social media platform, they enter a contractual relationship with said platform provider, thus activating rights both under the GDPR and the EU consumer law acquis. When signing up to a platform entails the processing of personal data, users become not only a data subject but also a consumer, as the consumer protection legal framework does consider one's data to be of economic value.[56]
Deployment of DPs such as stirring (emotional steering) or hindering (misleading information) at the moment of the sign-up process, thus the moment a user is about to enter into that contractual relationship with the platform provider, may also constitute an unfair commercial practice within the meaning of the Unfair Commercial Practices Directive.
BEUC recognizes the influence of such DPs on a user, which leads to an even greater information asymmetry[57] and can potentially be unfair and misleading and recommends including practices such as confirm-shaming (using emotion and language to steer users into certain actions) in the annex of banned practices of the UCPD.[58] This view is particularly important, taking into account the fast-paced nature of the internet and availability of vast resources and access to them through a simple click of the mouse. This type of direct and fast access eliminates a user's time for reflection and thus permits companies to exploit human impulses through emotionally triggering desired commercial actions.[59] As a result, these DPs may materially distort the economic behavior of the average consumer within the meaning of Article 5 UCPD

[52] Smith, A. Older Adults and Technology Use. (2014) *Pew Research Center*. Retrieved April ,13, 2022, from https://www.pewresearch.org/internet/2014/04/03/older-adults-and-technology-use/
[53] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 2020. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. In *CHI Conference on Human Factors in Computing Systems (CHI '20), April 25–30, 2020, Honolulu, HI, USA.* ACM, New York, NY, USA 14 Pages. https://doi.org/10.1145/3313831.3376600
[54] ibid.
[55] Bongard-Blanchy et al. 2021. "I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!" - Dark Patterns from the End-User Perspective. In Designing Interactive Systems Conference 2021 (DIS '21). Association for Computing Machinery, New York, NY, USA, 763–776. https://doi.org/10.1145/3461778.3462086
[56] Recital 24, European Parliament and Council Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1)
[57] The European Consumer Organisation. (2022). "DPs" and the EU consumer law acquis. Recommendations for better enforcement and reform. [Review of *"DPs" and the EU consumer law acquis. Recommendations for better enforcement and reform.*]. In *https://www.beuc.eu/publications/beuc-x-2022-013_dark_patters_paper.pdf*. p 9
[58] ibid p 13.
[59] Clifford, D. (2017) Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making, a True Path to the Dark Side?. CiTiP Working Paper Series, 31/2017. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3037425

and lead them to take a transactional decision which they would not have taken otherwise – in this context signing up to the social media platform. (**Urszula Baranowska + Thalis Cabral)**

25. As already highlighted by the EDPB Guidelines on consent, there must be a minimum information that users are provided with to meet the threshold of 'informed' consent.

According to Custers *et al.*, the basic model of consent consists of a two-step approach: (1) asking of consent by a data controller and (2) the providing of consent by a data subject.[60] With reference to the first step, the controller provides the necessary information to the user which will enable the user to decide. Custers *et al* advocates for this information to encompass both the content of consent (what is exactly consented to) and the process (how to consent) - in other words the way consent is to be given should be included in the minimum information threshold.[61] This can be done orally or in writing.

An example of how consent can be given in writing is when, during the sign-up process, the social media platform is provided with the user's email address. An email is sent to the user's email address by the social media platform containing the minimum information required to meet the threshold of 'informed' consent, as well as a step-by-step guide on how to consent online (or offline), for instance by clicking on a box or by submitting a form (which is very unlikely to be the preferred method due to the long turnaround time). The step-by-step guide should include information on where to find the minimum information and the privacy policy. The EDPB is invited to incorporate this process (how to consent) into the minimum information required to meet the threshold of 'informed' consent. **(Jasper Hille + Roberto de Alcântara)**

26. 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. As Article 7 (2) of the 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.

Overload of information. Situations in which users are confronted with excessive information on social media has been compared to '**overload**', which Fu et al. refers to '*an individual's subjective perception and evaluation of the number of information, people or objects that are beyond one's capability to process*',[62] which is what causes negative outcomes. Fu et al. refer that overload is caused by the so-called 'stressors', for instance, reading the T&Cs and privacy policies, with other stressors existing, such as placing information or UI elements in ways that users are not used to, or even the use of overly technical language.[63] The outcome of such stressors is **psychological exhaustion which leads to low participation and performance**,[64] which is not to be understood from the point of view of their use of the platform, but rather from how they reason from a psychological perspective. Thus, being presented with these stressors, leads to a user that is more susceptible, in this case to DPs. For instance, being presented with large amounts of overly technical language may lead the data subject from not reading at all the information that they are presented with,[65] which is problematic in the sign-up stage as the user is presented with several consent requests. Another factor to be taken into consideration in this reasoning is the one of '**social media fatigue'**

[60] Custers, B., van der Hof, S., & Schermer, B. (2014). Privacy expectations of social media users: The role of informed consent in privacy policies. *Policy & Internet, 6*(3)

[61] ibid.

[62] Fu, S. et al. (2020). Social media overload, exhaustion, and use discontinuance: Examining the effects of information overload, system feature overload, and social overload. Information Processing & Management, Volume 57, Issue 6, p.3. https://doi.org/10.1016/j.ipm.2020.102307

[63] ibid, p.5

[64] ibid, p.6

[65] Chromik, M. et al. (2019). DPs of Explainability, Transparency, and User Control for Intelligent Systems. IUI Workshops'19, p.3. http://ceur-ws.org/Vol-2327/IUI19WS-ExSS2019-7.pdf

which can be described as the '*tendency to back away from social media usage when they become over-whelmed with too many sites, too many pieces of content, too many friends and contacts and too much time spent keeping up with these connections'*.[66] This phenomenon may lead to already social media fatigued people to be more prone to not reading and/or blindly giving their consent as their tolerance has waned.
Considering research concentrating on such social media issues will allow to give a more well-defined threshold of information that can be presented to users before it being considered as excessive. **(Antonio Cannavacciuolo + Olga Lampousi)**

Unbundled consent. It should be reinforced that the mere opening of a social media account by a data subject does not equate to giving consent to the processing of the personal data of the data subject. A separate request for consent must be made to get consent from the data subject.
As an example, the company Enel was found guilty by the Italian DPA of processing the personal data of data subjects who had opened an account on their platform but who were not explicitly asked to give consent to sharing their data to third-party actors for targeted marketing purposes. Instead, the data subjects were merely asked to read the information on privacy in order to successfully open their account.[67] It should be clarified that **opening an account does not grant the platform the right to process data without consent,** particularly for the very intrusive purpose of targeted advertising. The platform should ask separately for the consent of its new user. (**Solène Tobler** + **Isabel Sierra Rubio**)

When is bundled consent permitted? Data controllers who bundle consent must demonstrate that they are not imposing disproportionate influence over the data subject's decision, even if they are making a take-it-or-leave offer. For example,

- the High Court of Frankfurt concluded that *"freely given consent is a consent that is given without coercion or pressure"*.[68]
- the Austrian Oberste Gerichtshof stated that the data controller must show the "*special circumstances in individual cases*" to ensure that bundled consent is freely given.[69]
- the Italian High Civil Court concluded that it is legal to bundle consent to the acceptance of marketing material where the service offered may be obtained through other ways and the data subject can renounce to it without a significant cost. However, if the data subject decides to exercise her right to withdraw, according to Article 7 (3) GDPR, controllers have an obligation to erase any data processed on the basis of consent provided that there is no other reason for continued retention.[70]**(Evangelia Cheiladaki + Eleni Arampatzi)**

> 31. Social network providers should therefore rely on means for security that are easier for users to reinitiate. 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. The controller should ensure a level of security appropriate to the risk for data subjects and the use of double factor authentication ("2FA") with SMS is precisely to protect data subjects from a

[66] Bright, L., Kleiser, S., Grau, S. (2015). Too much Facebook? An exploratory examination of social media fatigue. Computers in Human Behavior, Volume 44, p.149. https://doi.org/10.1016/j.chb.2014.11.048

[67] Garante per la Protezione dei Dati Personali, Ordinanza ingiunzione nei confronti di Enel Energia S.p.a. - 16 dicembre 2021 [9735672]
(Accessible online: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9735672)

[68] Van Quathem K. & Oberschelp de Meneses A. 2019. *German court decides that GDPR consent can be tied to receiving advertising.* https://www.insideprivacy.com/advertising-marketing/mobile/german-court-decides-that-gdpr-consent-can-be-tied-to-receiving-advertising/

[69] Oberste Gerichtshof, Decision No. 6 140/18h, Judgment of 31 August 2018, paras 4.44–4.45. (Austr.)

[70] European Data Protection Board. (2020). Consent Guidelines, *Adopted on 4 May 2020. May.*

data breach or phishing attacks.[71] The EDPB also suggests that e-mail versus SMS best suits the requirements of data minimisation.[72] Nevertheless, even if in principle the use of e-mail addresses seems less intrusive, it is up to controllers to determine whether they need to process personal data for their relevant purposes (in this case, security), since data minimisation comprises that the data must be necessary for the purposes they are processed.[73] Thus, SMS-based 2FA can be considered a safe method because protects 96% of bulk phishing attacks. The use of e-mail as the unique authentication method, on the other side, can be problematic since a password can easily be reset by e-mail, which means that in case of any security breach, an attacker must only compromise one factor of authentication, like an e-mail inbox, to take over the account.[74] In this sense, the Irish DPA fined a data controller for violations of Articles 5 and 32 of the GDPR precisely because it should have provided security regarding a leaked phishing e-mail scam.[75] One of the recommendations was exactly the implementation of 2FA for all users.[76] Thus, social network providers should consider the advantages or disadvantages of each type of 2FA depending on the concrete application[77] in high-risk situations to ensure cyber security, prevent phishing, and data breaches.[78]
(**Quezia Amaral Sayão + Stamatia Beligianni**)

> 32. 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.

Children. The guidelines seem to ignore the obligation stemming from Article 8(2) GDPR, requiring the data controller to "***make reasonable efforts to verify*** **whether children have parental authorisation to consent** for the data processing by, for example, a social media platform. Requiring signing up with a phone could be seen as such a reasonable effort, since it serves as proof that the user has a cell phone. If the user of the phone is a child, this means that "*the parents have at least agreed to the use of such a device and thus are aware that the child might sign up for such a service*".[79] This is especially the case in countries where registration and identification for using a SIM card is mandatory, which is the case in about half of EU member states.[80] This is important as methods that providers are currently using to establish age of consent, like forms where users have to report their underage use themselves, do not guarantee age verification.[81] Using this logic, requiring a phone number to sign up does fulfil the data minimisation principle, as the phone number is necessary for the platform to comply with Article 8(2) GDPR. The guidelines could

[71] Fowler, B. (2021, February 9). *The best way to use two-factor authentication*. Consumer Reports. Retrieved April 1, 2022, from https://www.consumerreports.org/digital-security/best-way-to-use-two-factor-authentication-a1070812070/

[72] Craddock, P., Millar, S. A., & Marshall, T. P. (2022, March 22). *EDPB on DPs: Lessons for marketing teams.* The National Law Review. Retrieved April 1, 2022, from https://www.natlawreview.com/article/edpb-dark-patterns-lessons-marketing-teams

[73] European Data Protection Board (2019) Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

[74] Robinson, K. (2021, July 18). *Is email based 2FA a good idea?* Twilio Blog. Retrieved April 2, 2022, from https://www.twilio.com/blog/email-2fa-tradeoffs

[75] Brennan, C., & McConnell, D. (2022, January 17). *Teaching Council fined €60,000 after teacher data leaked in phishing scam.* Irish Examiner. Retrieved April 2, 2022, from https://www.irishexaminer.com/news/arid-40787280.html

[76] Teaching Council x Data Protection Commission, DPC Case Reference: IN-20-4-1, (2021, 2 December) Retrieved April 2, 2022, from https://www.dataprotection.ie/sites/default/files/uploads/2022-01/Redacted%20Final%20Decision%20The%20Teaching%20Council_20-04-01.pdf para 8.7

[77] Fowler, B. (2021, February 9). *The best way to use two-factor authentication*. Consumer Reports. Retrieved April 1, 2022, from https://www.consumerreports.org/digital-security/best-way-to-use-two-factor-authentication-a1070812070/

[78] Denayer, D. (2021, September 27). *Use Two-factor authentication to comply with GDPR*. OneSpan. Retrieved April 1, 2022, from https://www.onespan.com/blog/use-two-factor-authentication-comply-gdpr

[79] Schneble, C. O., Favaretto, M., Elger, B. S., & Shaw, D. M. (2021). Social Media Terms and Conditions and Informed Consent From Children: Ethical Analysis. *JMIR Pediatrics and Parenting*, *4*(2), 1–12. https://doi.org/10.2196/22281, p. 6.

[80] GSM Association. (2021, April). *Access to Mobile Services and Proof of Identity 2021 - Revisiting SIM Registration and Know Your Customer (KYC) Contexts during COVID-19.* https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf, p. 60-61.

[81] ibid.

elaborate on whether or not this practice is acceptable, and if not how a company is supposed to fulfil the obligations from Article 8(2). (**Tomas Baçe + Arystan Jazin)**

The Guidelines seem to imply that authentication is used only for the purpose of data subjects being able to log into the social network or when registering. Authentication is used throughout the entire customer life cycle. For instance, online providers may request a user to authenticate him/herself when: i) registering for an application; ii) logging in; iii) retrieving a forgotten password; iv) changing an existing password; v) deleting an account.[82] Service providers may also request authentication for other goals which could include a request by the data subject to access his/her data. Request for authentication for SAR has been also addressed in paragraph 63, 65, 70, 71, 72, 73, 74 and 76 of the recent Draft Guidelines 01/2022 on data subject rights - Right of access. Perhaps a distinction could be made by the EDPB between service providers which use one-time-verification vs those that use verification more than once. **We consider that the EDPB should further elaborate and explain in this paragraph that authentication can be used not only for the purpose of logging into or registering into a social network but also for other purposes**. (**Magdalena and Elena**)

Comment 2: The current Guidelines seem to suggest that providers should limit themselves to use only email for the purpose of authentication and refrain from using SMS authentication due to its intrusiveness (*see paragraph 31 of these Guidelines*). A stronger authentication can facilitate protection and verify the identity of the user. A double verification system is recommended, where the company's system can generate a one-time unique code which will be sent to the user's mobile phone number in order to verify the user's identity. The Guidelines also seems to reference to the possibility to perform a double verification (e.g., use of email and use of phone number). (**Magdalena and Elena**)

> 39. With the Emotional Steering DPs, wordings or visuals are used in a way that conveys information to users in either a highly positive outlook, making users feel good or safe, or a highly negative one, making users feel anxious or guilty.

Emotional steering can be strong during the sign-up process also due to a common practice from Facebook, that the Norwegian Consumer Council named as **‘*Reward and Punishment*’**.[83] This strategy regards either the recompense of users if they opted for a correct choice, granting them an improved user experience, or their punishment if they opted for an undesirable choice, such as a refusal of tracking.[84] This means that the platform influences data subjects to opt for what it considers as a correct choice, especially through offering ‘*variable rewards’* in order for the service to be able to ‘create an appetite, a desire’ as CNIL mentions[85], ‘*sufficient enough to incite consumers to carry on’*.[86] Such desire is triggered when platforms **use social benefits such as ‘*virtual badges’*** to control data subjects’ actions and behavior. For instance, a location sharing application called Foursquare offers to the users who ‘check in’ at a specific place the most, a **‘*mayor***

[82] This had been discussed during the webinar ” Frictionless Biometric Authentication under PSD2 and GDPR Regulation” which was conducted by Simon Moffatt and Gal Steinberg, <https://www.thecyberhut.com/frictionless-biometric-authentication-under-psd2-and-gdpr-regulation/?utm_source=rss&utm_medium=rss&utm_campaign=frictionless-biometric-authentication-under-psd2-and-gdpr-regulation> accessed 14 April 2022.

[83] Forbrukerrådet (Norwegian Consumer Council). 2018. Deceived By Design: How Tech Companies Use DPs to Discourage Us from Exercising Our Rights to Privacy. Report. 1-43, p. 25.

[84] Gray, Colin M., Cristiana Santos, Nataliia Bielova, Michal Tóth and Damian Clifford. 2021. DPs and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. doi: 10.1145/3411764.3445779: 1-18, p 11.

[85] CNIL. Shaping Choices in the Digital World-From DPs to data protection: the Influence of UX/UI Design on User Empowerment. 2019. LINC. IP Reports. Innovation and Foresight. N° 06. 1-48, p. 17.

[86] CNIL Report, p. 18.

***badge*'.**[87] On the other hand, an example of punishment is the increase of costs or the creation of extra barriers when selecting '*specific configurations'*, hampering users of no technical expertise to opt for 'risky settings'.[88] 'Reward or Punishment' constitutes a practice that can affect to a large extent the emotional behavior of the data subjects nudging them to take or change a decision, a choice they would otherwise not opt for. Thus, in order to grant more protection to data subjects, the EDPB may consider including in their Guidelines this particular social media platform strategy, since it can be linked directly with DPs based on emotional steering. **(Antonio Cannavacciuolo + Olga Lampousi)**

Vulnerable groups. The 'vulnerable nature' of data subjects is an important concept that needs to be focused in the context of vulnerable people, such as the **elderly, those with cognitive impairments, and people who are visually impaired**.[89]
The ICO defined vulnerability as instances where individuals' capacity may be hindered to freely agree or object to the processing of their personal data (in this case at the registration stage), or to comprehend the ramifications.[90] The use of emotional steering could influence vulnerable individuals, such as the elderly or those with cognitive impairments, through wording and visuals to provide more information than is necessary since it may give them a feeling that it is good or safe. Focusing in particularly on the elderly, according to a study by *Bongard-Blanchy et al*, the older generation is less capable of detecting manipulative tactics (DPs), but they also are less conscious that their decisions or behavior can be influenced. For this reason, the use of DPs is especially harmful for older persons, as they struggle to adapt their taught self-protection capabilities to developing (digital) environments due to a combination of lack of awareness and capability.[91] As a result, it would be beneficial if social media platform services were to adopt a standard practice to ensure special protection of vulnerable people, an example of a similar practice would be Recital 38 of the GDPR that provides for specific measures to protect children's rights. In this way, these specific measures can be adapted to fit the vulnerable context, and ensure that vulnerable persons, such as the elderly, are not as susceptible to being emotionally persuaded into sharing more information. **(Urszula Baranowska + Thalis Cabral)**

Fear of Missing Out in the sign-in process. Emotional Steering integrated in social media platform interfaces can result in the development of FoMO-Centric platforms-- **Fear of Missing Out ('FoMO')**[92] is "*a pervasive apprehension that others might be having rewarding experiences from which one is absent*". Przybylski et al. found that FoMO can lead users to act in a detrimental way to their privacy and security, despite being aware of the negative effects.[93] The phenomenon of FoMO seems to be relevant to social media engagement and has been presented as a 'mediator' associating psychological needs deficits with the use of social media.[94] Therefore, it seems that platform interfaces exploit users' vulnerabilities and their

[87] Alessandro Acquisti et al. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. 2017. ACM Comput. Surv. 50. https://doi.org/10.1145/3054926 : 44:1–44:41, p. 44:22.
[88] Alessandro Acquisti et al, p. 44:22.
[89] Piasecki, S. and Chen, J, 'Complying with the GDPR when vulnerable people use smart devices' (2022) International Data Privacy Law <https://doi.org/10.1093/idpl/ipac001> accessed, 11 April 2022 2.
[90] Information Commissioner's Office, 'When Do We Need to Do a DPIA?' < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when11> accessed, 10 April 2022
[91] Bongard Blanchy et al, 'I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!" - DPs from the End-User Perspective' (Designing Interactive Systems Conference, Virtual Event, 2021) <*https://doi.org/10.1145/3461778.3462086*> accessed, 14 April 2022 773.
[92] Westin, F. (2020). Fomo-Centricity: How Social Media's Dark Designs Cause Users to Reluctantly Give Up Their Data. Carleton University, 9.
[93] Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. Computers in Human Behavior, 29(4), 1847. https://doi.org/10.1016/j.chb.2013.02.014
[94] Wastin, F., Chiasson, S. (2019). Opt Out of Privacy or "Go Home": Understanding Reluctant Privacy Behaviours through the FoMO-Centric Design Paradigm. Association for Computing Machinery, 57-67. https://doi.org/10.1145/3368860.3368865

need for ‘connecting’ with others in order to accomplish their goals and hence behave contrary to the principle of fairness.

Concerning the signing up process, platforms can force users to reveal more personal data by triggering their automatic and unconscious thinking.[95] This may have negative impacts to users’ privacy behaviours as users tend to act in a way they would not if they were in a more deliberate mindset during the signing up process. We consider that the Guidelines should tackle this issue by eliminating the FoMO-centric designs and enhancing the formulation of private-centric platform interfaces. **(Evangelia Cheiladaki + Eleni Arampatzi)**

40. 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** (i.e. provide more personal data due to lack of understanding of processing activities), considering their “vulnerable nature” as data subjects. When social media platform services are addressed to children, they should ensure that the language used, including its tone and style, is appropriate so that children, as recipients of the message, easily understand the information provided. Considering the vulnerability of children, the DPs may influence children to share more information, as “imperative” expressions can make them feel “obliged” to do so to “appear popular among peers”.

Children. One in three internet users around the world is a child before the age of 18.[96] According to an empirical study by Smahel *et al* from 2020, 54% of the children aged 9 to 16 visit social media at least once a day.[97] Despite Article 8 GDPR, which requires parental consent when personal data of children is processed, 28% of children aged 9 to 11, 63% of children aged 12 to 14, and 77% of children aged 15 to 16 visit social media daily.[98] Privacy and confidentiality are key aspects to children's holistic and healthy development.[99] The ICO suggests that for very young kids (up to 9 years of age) explanations should be simplistic, while for kids in their early teens (13-15) **explanations of functionality and inherent risk are suggested**.[100] Children from the age of 6 onwards may start being more susceptible to peer pressure because the need to fit in with their peer group becomes more important.[101] While research by Graßl *et al*.[102] indicates pro-privacy nudges (such as bright patterns) can work, teaching behaviours and skills would have longer lasting effects (which is further corroborated by research on the positive learning effect of gamification elements in social media environments on teenagers by Alemany, Val and Garcia-Fornes[103]). However, practical concerns about the feasibility of introducing such nudges remain. Still, the EDPB should not just be clear about the dangers of Emotional Steering to children (of varying ages), but also address the positive

[95] Westin, F., Chiasson, S. (2021). “It’s So Difficult to Sever that Connection”: The Role of FoMO in Users’ Reluctant Privacy Behaviours. Association for Computing Machinery, 550, 1-15.

[96] UNICEF. (2017, december). Children in a Digital World, The State of the World’s Children 2017 (ISBN 978–92-806-4938-3). UNICEF Division of Communication. https://www.unicef.org/media/48601/file, p.7.

[97] Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries*. EU Kids Online. Doi: 10.21953/lse.47fdeqj01ofo, p. 29.

[98] Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries*. EU Kids Online. Doi: 10.21953/lse.47fdeqj01ofo, p. 30.

[99] UNICEF. (2017, december). Children in a Digital World, The State of the World’s Children 2017 (ISBN 978–92-806-4938-3). UNICEF Division of Communication. https://www.unicef.org/media/48601/file, p.7.

[100] Information Commissioner’s Office. (2020, September). *Age appropriate design: a code of practice for online services* (2.1.128). https://ico.org.uk/media/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf, p. 75.

[101] Information Commissioner’s Office. (2020, September). *Age appropriate design: a code of practice for online services* (2.1.128). https://ico.org.uk/media/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf, p. 98.

[102] Graßl, P., Schraffenberger, H., Zuiderveen Borgesius, F., & Buijzen, M. (2021). Dark and Bright Patterns in Cookie Consent Requests. Journal of Digital Social Research, 3(1), 1-38. https://doi.org/10.33621/jdsr.v3i1.54.

[103] J. Alemany, E. D. Val and A. Garcia-Fornes, "Assessing the Effectiveness of a Gamified Social Network for Applying Privacy Concepts: An Empirical Study With Teens," in IEEE Transactions on Learning Technologies, vol. 13, no. 4, pp. 777-789, 1 Oct.-Dec. 2020, doi: 10.1109/TLT.2020.3026584.

influence nudging could have to help children make the best choices - decreasing the chance of Emotional Steering and in adherence with the principle of fairness of processing. (**Jasper Hille + Roberto de Alcântara**)

Children. To stay connected, most young users feel the pressure to stay connected and to fit in with their peers[104]. It is understood that article 8 and 12 of the GDPR offer specific protection, and that parental authorization is required for users under the age of 13-16, however, it must be considered that in some cases, this is not the most effective way to obtain consent since it can be easy for young users to not be truthful and to ***bypass*** this requirement.[105] Suggestions by other stakeholders could be seconded by the EDPB:

- Consumentenbond[106] (report on Children and Data Protection) for social media platforms to create separate information processing addressed to children that is straightforward, easy to read and not long (long phrases and difficult terminology will also discourage children from reading the policy). One way this can be done is through **audio-visual aids, such as animation or graphic design with audio recording, in which the risks, consequences, and safeguards are clearly explained**.[107]
- ICO transparent approach and to bring awareness of the risks, consequences, and safeguards for the child to make an informed decision.[108] **Urszula Baranowska + Thalis Cabral)**

Parental portals. It has become difficult for children to refuse to be part of social media, because of both social pressure and an increasing number of institutions such as schools requiring communication through such channels, resulting in social pressure to use these services for communication, regardless of whether parents regard its use as appropriate for their children.[109]
A report from the UK Children's Commissioner[110] has shown that the safe use of these social media services depends on building awareness and educating children about its use and encouraging digital literacy.[111] Most apps offer **parents websites** where the companies either provide links to useful literature or by providing short YouTube videos to inform children and parents about the potential harms and security measures to take when using social media.[112] Schneble *et al.* suggests implementation of such **parental portals**,[113]perhaps in the form of a link designed into the sign-up box of the social media platform. This suggestion could encourage platfroms to spend resources in educating parents and children about the potential harms resulting from dark patterns.[114] **(Jasper Hille + Roberto de Alcântara)**

[104] Eveline A. Crone, Elly A. Konijn, 'Media use and brain development during adolescence' (2018) 9 Nat Commun <https://www-nature-com.proxy.library.uu.nl/articles/s41467-018-03126-x.pdf> accessed, 12 April 2022

[105] Dorine Dollekamp and Tommy Fitzsimons, 'Children and Data Protection' (Consumentenbond, 2021) <https://ilplab.nl/wp-content/uploads/sites/2/2021/04/Rapport-Children-and-Data-Protection-Justification.pdf > accessed, 12 April 2022 4.

[106] Ibidem

[107] Dorine Dollekamp and Tommy Fitzsimons, 'Children and Data Protection' (Consumentenbond, 2021) < https://ilplab.nl/wp-content/uploads/sites/2/2021/04/Rapport-Children-and-Data-Protection-Justification.pdf > accessed, 12 April 2022 16.

[108] Information Commissioner's Office (ICO), 'What should our general approach to processing children's personal data be?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/what-should-our-general-approach-to-processing-children-s-personal-data-be/> accessed, 13 April 2022

[109] Schneble, Christophe Olivier, et al. "Social Media Terms and Conditions and Informed Consent From Children: Ethical Analysis." *JMIR pediatrics and parenting* 4.2 (2021): e22281.

[110] Butterfill R, Charlotte M-P, Powell H, Nettleton O, Kriszner M. Life in Likes: Children's Commissioner Report into Social Media use in among 8-12 Year Olds Internet. *UK Children's Commissioner*. 2018. [2020-07-01]. https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/01/Childrens-Commissioner-for-England-Life-in-Likes-3.pdf.[Ref list]

[111] Schneble, Christophe Olivier, et al. "Social Media Terms and Conditions and Informed Consent From Children: Ethical Analysis." *JMIR pediatrics and parenting* 4.2 (2021): e22281

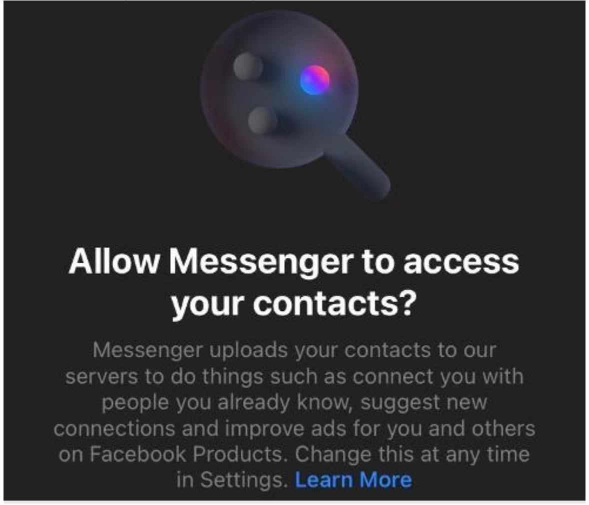
[112] ibid.

[113] ibid.

[114] ibid.

41. 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.

Optimism bias and syncing contacts. A user may provide more data than required not only because she is under time pressure or believes that is what other users would do but also due to the **'optimism bias'**. Such bias needs to be included in the guidelones. Optimism bias refers to the tendency to think that one is less likely to experience online privacy risks than others.[115] An example refers to ***syncing contacts*.** Facebook Messenger uses this message for asking users to sync their contacts:



Allow Messenger to access your contacts?

Messenger uploads your contacts to our servers to do things such as connect you with people you already know, suggest new connections and improve ads for you and others on Facebook Products. Change this at any time in Settings. Learn More

The expressions '*connect you with people you already know*', '*suggest new connections'*, and '*improve ads for you*' suggest something very positive, which is in contrast with the reality behind syncing contacts. Namely, this enables Facebook to upload a list of people that the user knows, use that information to show her ads, and share the information with Facebook-owned apps.[116] This practice's intrusiveness is exacerbated by the fact that smartphone usage features such as the average number of calls or SMS could predict personality traits,[117] and all of this information may, in turn, be used for targeted advertising. And yet, users may be overly optimistic and consider Messenger to be just a tool for texting their friends. Considering this, if the Guidelines strive to increase users' awareness of the risks possibly coming from sharing too many data, an explanation of the optimism bias should be provided, and given the possible implications of syncing contacts, it might be appropriate to use this example for illustrating its exploitation. (**Eva Opsenica + Joanna Taneva**)

Knowledge of user's vulnerabilities. Another form of emotional steering could take place if social media platforms were to **combine the knowledge of a user's emotional state, with a fitting message**. Social media companies that use targeted tracking and advertising, may have information **regarding a user's vulnerabilities**, and have data driven approaches to best persuade each individual user. Facebook, for

[115] Cho, H., Lee J., & Chung S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human* Behavior, *26(5)*, 987-995, 992. https://doi.org/10.1016/j.chb.2010.02.012

[116] Bell, K. (2019, 1 August). Stop syncing your contacts with Facebook. *Mashable*. https://mashable.com/article/stop-syncing-contacts-with-facebook

[117] Castelluccia, C. (2020, July 22). From Dataveillance to Datapulation: The Dark Side of Targeted Persuasive Technologies. hal-02904926. 6. https://hal.archives-ouvertes.fr/hal-02904926

example, knows its users to such a degree that it knows their individual vulnerabilities.[118] With the extensive knowledge of their users, Facebook enables advertisers to use, for example low self-esteem, fears or financial difficulties, to influence behaviour.[119] However, if a company like Facebook were to use this knowledge to use fitting motivational language as persuasion to have the user "consent" for their data to be used, this could lead to emotional steering even more effective than a standard message for everyone.
Therefore, guidance regarding the use of already collected personal information (and personal vulnerabilities) by a company in consent requests would be helpful for clarification. Clarification is needed in regard to the validity of consent, in a case where a social media platform, for example, changes its consent request language based on its knowledge on a user's mental illness, or elderly status, even if the language itself does not necessarily constitute emotional steering to most people. **(Tomas Baçe + Arystan Jazin)**

42. During the sign-up process stage, the users' goal is to complete the registration in order to be able to use the social media platform. DPs such as **Emotional Steering** have stronger effects in this context.

A given platform design should apply "**reflective**" patterns, slowing down the process and giving the user more time to think about their decisions and impact on their privacy, as opposed to optimizing the interface for less clicks and less time. This could be done through several strategies which are outlined in variety of academic literature, for example

- deliberately slowing down the process or breaking it up into more components to avoid risk-taking behavior, *Distler et al (2020)*[120]
- challenging one's habitual behaviors and thoughts to provide contrasting perspectives and opinions, *Vasalou et al*[121]
- ask the user specific questions in order to force the user to consider other perspectives, *Broockman and Kalla (2016)*[122]

Proponents of such "slow" or "reflective" design theories underline the benefits for individuals and society of a more mindful usage of social media and their continuous reflection of its impact on one's privacy. Therefore, the design of the sign-up process needs to counter the rush and susceptibility of users to the sense of urgency and encourage reflection in such non-repetitive requests for data.[123] **(Urszula Baranowska + Thalis Cabral)**

46. 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*** DPs 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

[118] Bol, N., Strycharz, J., Helberger, N., van de Velde, B., & de Vreese, C. H. (2020). Vulnerability in a tracked society: Combining tracking and survey data to understand who gets targeted with what content. *New Media & Society*, 22(11), 1996–2017, p. 1999.

[119] Ibidem, p. 2000-2001.

[120] Distler, V., Lenzini, G., Lallemand, C., & Koenig, V. (2020, October). The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely. In New Security Paradigms Workshop 2020 (pp. 45-58).

[121] Vasalou, A., Oostveen, A.-M., Bowers, C., Beale, R., 2015. "Understanding engagement with the privacy domain through design research," Journal of the Association for Information Science and Technology, volume 66, number 6, pp. 1,263–1,273.

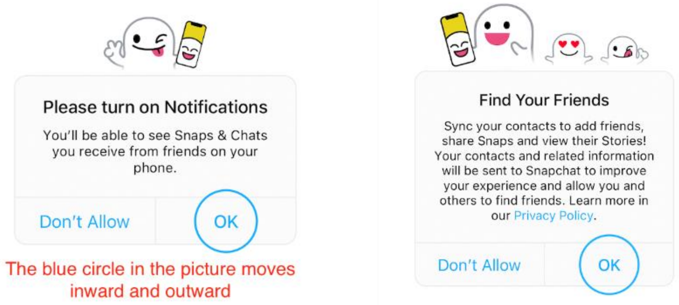
[122] Broockman, D., Kalla, J., 2016. "Durably reducing transphobia: A field experiment on door-to-door canvassing," Science, volume 352, number 6282 (8 April), pp. 220–224.

[123] Terpstra, A., Schraffenberger, H., & Graßl, P. (2020). *Think before you click: how reflective patterns contribute to privacy* [Review of *Think before you click: how reflective patterns contribute to privacy*]. Radboud Repository. https://repository.ubn.ru.nl/bitstream/handle/2066/246490/246490.pdf?sequence=1&isAllowed=y

Balanced choices. In addition to violating the fairness principle, this scenario amount to an invalid consent. Namely, this violates the requirement of an unambiguous indication of wills as prescribed by Article 4(11) read in conjunction with Article 7(3) GDPR. Indeed, data subjects are not provided with a balanced choice (ie. for consenting only one click is required, while for rejecting two clicks are required). The balanced choice has been recognized by A-G Szpunar under the Planet49 Decision ("actions must, optically in particular, be presented on an equal footing").[124] Third, several DPAs (eg. the UK DPA)[125] have emphasized the importance of the requirement. (**Rijk Rouppe van der Voort**)

47. 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.

Motion. It would be beneficial for the EDPB to also take into consideration the use of motion when dealing with interface-based patterns. Research shows that 'motion onset', which is the first stage of motion, is able to strongly capture the attention of an individual,[126] and therefore it can be inferred that it can be used to nudge the attention, and subsequent action of a data subject. An example of this usage of motion can be found during the sign-up procedure of Snapchat in which a brightly colored moving circle is placed around the 'OK' selection for accepting the platform's notifications and the syncing of the data subject's contacts with the app. Such use of a moving circle is indeed capable of capturing one's attention for that specific selection, allowing consent to receive notifications and share contacts. **(Antonio Cannavacciuolo + Olga Lampousi)**



Please turn on Notifications

You'll be able to see Snaps & Chats you receive from friends on your phone.

Find Your Friends

Sync your contacts to add friends, share Snaps and view their Stories! Your contacts and related information will be sent to Snapchat to improve your experience and allow you and others to find friends. Learn more in our Privacy Policy.

Figure - The video of the moving circle can be seen at https://imgur.com/a/lq0bR8V

X Button. An example of a bait and switch DP can be found in the case of Microsoft and their recommended update for Windows 10, Microsoft did not use the X button in the top right of the screen in the traditional method and instead chose to have it act as a tool for permitting the update to occur.[127] This is an evident bait and switch as users are naturalized to thinking that the X button is the close button[128]. The way this can translate into social media is through if they ask you for consent, and you choose not to, however, in a later screen you find out that the button in fact was indeed the button that permits the granting of consent. By

[124] Opinion of Advocate General Szpunar on the case of Planet49 (Case C-673/17), delivered on 21 March 2019 at para 66, https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:62017CC0673, accessed 14 April 2022.

[125] Information Commissioner's Office (2019), "Guidance on the use of cookies and similar technologies" Privacy and Electronic Communications Regulations at 32, https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf accessed 14 April 2022.

[126] Abrams, R. A., Christ, S. E. (2003). Motion Onset Captures Attention. Psychological Science, 14(5), 427–432, p.431. https://doi.org/10.1111/1467-9280.01458; *See* also Smith, K.C., Abrams, R.A. (2018). Motion onset really does capture attention. *Atten Percept Psychophys* 80**,** 1775–1784, p. 1728. https://doi.org/10.3758/s13414-018-1548-1

[127] Brignull, H. (n.d.). Bait and switch - a type of deceptive design. Deceptive Design. https://www.deceptive.design/types/bait-and-switch

[128] Jaiswal, A. (2017). DPs in UX Design. *Information Professions*, 1–14. Retrieved 2017, from https://irenelopatovska.files.wordpress.com/2018/03/dark-patterns-in-ux-design-assignment-3-arushi.pdf.

having such an option present, it may present itself as an issue as without the specific mentioning of such a term as bait and switch. (**Tomas Baçe + Arystan Jazin)**

Muscle memory. The EDPB should pay particular attention to the deception technique, which Brignull describes as a "Bait and Switch"[129], in concrete, the "muscle memory". Muscle memory is a form of procedural memory in which a specific motor task is consolidated in memory through repetition.[130]The recent Instagram update (2020) created a new layout, moving options for camera and notifications to the top part and introducing new options (Reals and Shop) in their place. With that in mind, users now have a higher likelihood of unintentionally clicking on new options, simply relying on the repetitive function of their fingers nudging them to the same spot where other options previously existed.[131]Therefore, it should be advisable for the EDPB to include this type of manipulative and deceptive technique in the Guidelines. **(Dušan Stevanović)**

48. **Using small font size or using a colours which do 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.

Location-based DPs. From empirical evidence, 'location-based DPs' also constitutes a manipulative technique designers use to coerce and trick data subjects to agree to policies that most of them would not accept in other cases.[132] These location-based DPs can be identified when the agree button is placed where the 'Next step' or 'Continue' button is usually placed.[133] Because of how this visual pattern operates, and its inherent manipulation of the data subject's muscle memory stemming from using other websites, this visual trick violates the principles of fairness and lawfulness of Article 5 of the GDPR, and the 'freely given consent' requirement under Article 7 in conjunction with Article 4 (11) of the GDPR. **(Antonio Cannavacciuolo + Olga Lampousi)**

Icons (Exampe 8). Icons[134] can be used as a steering component[135] and represent hidden in plain sight DPs. Namely, companion icons[136] can significantly enhance the readability and understanding of information, as several studies showed.[137] But when used for the opposite purpose they can negatively affect users when the design is such. For instance, in the depicted Figure[138] there are bulb icons accompanying textual information.

[129] Gray C. M., Kou Y., Battles B., Hoggatt J., and Toombs A. 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)*. dl.acm.org, 534:1–534:14. https://doi.org/10.1145/3173574.3174108

[130] DC Vesser, *(Just About) Everything You Should Know About A Handgun*, (First Edition, Page Publishing Inc, 2018)

[131] Mariana Vargas, 'Is the New Instagram Update a New Form of Dark Pattern?' (UX Planet, 19 November 2020) <https://uxplanet.org/is-the-new-instagram-update-a-new-form-of-dark-pattern-1776697cffd8> accessed 17 April 2022

[132] Colin, M. G., et al. End User Accounts of DPs as Felt Manipulation. 2021. Proceedings of the ACM on Human-Computer Interaction 5, CSCW2, 372:1–372:25, p. 372:11.

[133] Colin, M. G., et al. p. 372:11.

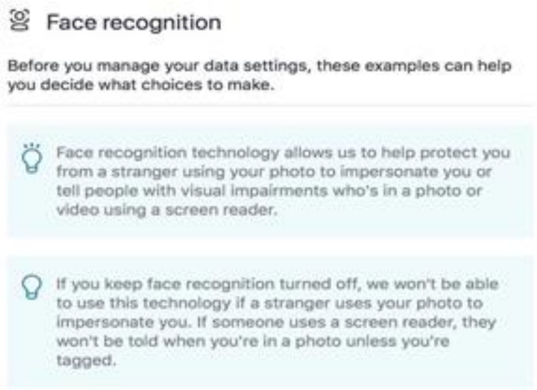
[134] Haapio, H. & Passera, S. 2016. Contracts as interfaces: Exploring visual representation patterns in contract design. In M. J. Katz, R.A. Dolin & M. Bommarito (Eds.) Legal Informatics, Cambridge, UK: Cambridge University Press. Published ahead of print as part of doctoral dissertation, 37 pages, page 26-27.

[135] Arianna Rossi, Monica Palmirani, „DaPIS: An Ontology-Based Data Protection Icon Set", Knowledge of the Law in the Big Data Age G. Peruginelli and S. Faro (Eds.) © 2019 The authors and IOS Press. This article is published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License 4.0 (CC BY-NC 4.0). doi:10.3233/FAIA190020, page 184.

[136] Arianna Rossi, Monica Palmirani, DaPIS: a Data Protection Icon Set to Improve Information Transparency under the GDPR, January 21, 2019. page 39.

[137] Passera, S. (2015). Beyond the Wall of Text: How Information Design Can Make Contracts User-friendly. In International Conference of Design, User Experience, and Usability. Springer, 341-352., page 348.

[138] Arianna Rossi, Presentation held within Data Protection Course – Law and Technology in Europe.



Face recognition

Before you manage your data settings, these examples can help you decide what choices to make.

Face recognition technology allows us to help protect you from a stranger using your photo to impersonate you or tell people with visual impairments who's in a photo or video using a screen reader.

If you keep face recognition turned off, we won't be able to use this technology if a stranger uses your photo to impersonate you. If someone uses a screen reader, they won't be told when you're in a photo unless you're tagged.

Screenshot– Companion icon – Bulb

Although the textual information itself can be considered as a DPs, an additional DPs can be seen in the icons - the icon accompanying the allowing option is a switched-on bulb, while a switched-off bulb follows the option denying consent. Designers purposely choose bulb icons, not as a turn-on/turn-off option yet as a form of "hidden in plain sight" pattern to steer users to give data. The definition of light-bulb moment represents "a moment when you suddenly realize something or have a good idea".[139] Additionally, some scholars examined how common metaphors, including "light bulb", about ideas would impact judgments about ideas and the people who have them. The study showed that metaphors about ideas influence judgments of idea quality.**[140]-**[141] Thus, usage of the metaphorical interfaces concerning an icon as companion, should be observed in the Guidelines. **(Marina Mijušković)**

51**.** Social media providers also need to be mindful of the principle of data protection by default. When data settings are **preselected**, 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.

Privacy dashboards. Bonneau *et al.*[142] estimates that between 80 to 99% of users are found to never change their privacy settings[143]and a further considerable number of users estimated at 26 %[144] and 30%[145] are not even aware that privacy controls exist in social networks.

Definition of light-bulb moment from the Cambridge Advanced Learner's Dictionary & Thesaurus © Cambridge University Press), available on https://dictionary.cambridge.org/dictionary/english/light-bulb-moment .

[140] Zahar Koretsky, "Phasing out an embedded technology: Insights from banning the incandescent light bulb in Europe",Maastricht University Science, Technology and Society (MUSTS) Group, Faculty of Arts and Social Sciences, Maastricht University, The Netherlands, Elsevier, Energy Research & Social Science 82 (2021) 102310, page 3.

[141] Kristen C. Elmore, Myra Luna-Lucero , "Light Bulbs or Seeds? How Metaphors for Ideas Influence Judgments About Genius", Social Psychological and Personality Science 2017, Vol. 8(2) 200-208, page 201-202.

[142] Bonneau, J., & Preibusch, S. (2010). The privacy jungle: On the market for data protection in social networks. In *Economics of information security and privacy* (pp. 121-167). Springer, Boston, MA.

[143] Acquisti, A., & Gross, R. (2006, June). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies*(pp. 36-58). Springer, Berlin, Heidelberg; Krishnamurthy, B., & Wills, C. E. (2008, August). Characterizing privacy in online social networks. In *Proceedings of the first workshop on Online social networks*(pp. 37-42).

[144] Harvey Jones and Jose Hiram Soltren. Facebook: Threats to privacy. *http://web.mit.edu/jsoltren/www/facebook.pdf*, 2005.

[145] Acquisti, A., & Gross, R. (2006, June). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies*(pp. 36-58). Springer, Berlin, Heidelberg

The report of Kristina Irion *et al.* suggests the use of privacy dashboards as a practical solution to enhance user control and ensure the protection of data.[146]-[147] Theoretically, privacy dashboards can be designed to meet privacy by design and usability criteria.[148] Considering the above, the EDPB could recommend the use of privacy dashboards for users to avoid preselected choices. (**Jasper Hille + Roberto de Alcântara**)

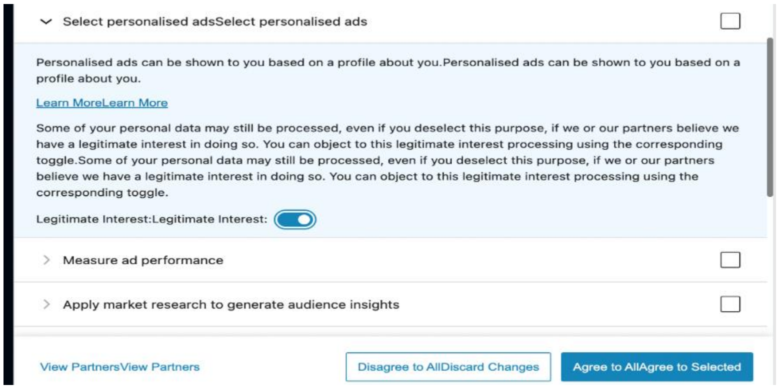
> 52. When the most data invasive features and options are enabled by default, this constitutes the dark pattern Deceptive Snugness.
> **Example 9:** In this example, when users enter their birthdate, they are invited to choose with whom to share this information.

Preselection. In 2017 the Article 29 Working Party Guidelines had already made clear that "the use of pre-ticked opt-in boxes is invalid under the GDPR".[149] This interpretation was later confirmed in *Planet* 49 (2019), where the court held a pre-ticked box does not constitute valid consent.[150] Therefore, one could ask the question what the benefit of adding a whole category called "deceptive snugness" is, when this essentially entails pre-ticked boxes or preselection, which are already deemed to be incompatible with the GDPR in the first place. Guidelines are useful for providing clarifications, however, the problem that arises here is that adding an extra category might cause more questions than it provides for clarity.
(**Tomas Baçe + Arystan Jazin)**

> 53. This is a Deceptive Snugness pattern, as it is not the option offering the highest level of data protection that is selected, and therefore activated, by default. 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.
>
> 55.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.

Preselection of Legitimate interest legal basis. Sometimes, the data processing based on 'legitimate interest' mentioned in Art.6(f) GDPR may constitute deceptive sulgnes when website designs take it as the default (like the example below), when actually conent is the correct ground (personalized ads), causing users can hardly notice let alone change, the default settings. Thus, there is the risk of preventing users from exercising their right (Recitals 69-70) to object to the vendor's declaration of Legitimate Interest. This is a very recurrent practice that the gudelines cannot afford to miss. (**Dina Kristina Denso+ Shuoyuan Jiang)**

[146] Irion, Kristina, et al. "A roadmap to enhancing user control via privacy dashboards." (2017).
[147] ibid. See also: Zimmermann, Christian, Rafael Accorsi, and Günter Müller. "Privacy dashboards: reconciling data-driven business models and privacy." *2014 Ninth International Conference on Availability, Reliability and Security*. IEEE, 2014.
[148] ibid.
[149] European Commission. (2017, October). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (wp248rev.01). https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711, p. 16.
[150] C-673/17 Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH ECLI:EU:C:2019:801, para 63.



Select personalised adsSelect personalised ads □

Personalised ads can be shown to you based on a profile about you.Personalised ads can be shown to you based on a profile about you.

Learn MoreLearn More

Some of your personal data may still be processed, even if you deselect this purpose, if we or our partners believe we have a legitimate interest in doing so. You can object to this legitimate interest processing using the corresponding toggle.Some of your personal data may still be processed, even if you deselect this purpose, if we or our partners believe we have a legitimate interest in doing so. You can object to this legitimate interest processing using the corresponding toggle.

Legitimate Interest:Legitimate Interest: ●

Measure ad performance □

Apply market research to generate audience insights □

View PartnersView Partners
Disagree to AllDiscard Changes
Agree to AllAgree to Selected

Tumblr: <https://www.tumblr.com/privacy/consent/beginredirect=https%3A%2F%2Fwww.tumblr.com%2Fpolicy%2Fprivacy >, accessed 14 April 2022

Example 10: Users are not provided with any links to data protection information once they have started the sign-up process.

Uninformed consent. The information must be provided in clear and plain language that is easily understandable for the average person.[151] However, if the data subject is not provided with information that he is looking for and subsequently completes his registration because he has no other option, as exemplified by paragraph 57 of the EDPB Guidelines, this seems to constitute an **uninformed** consent. Therefore, it is recommended that the EDPB includes this element in the explanation of the ***Dead end*** DPs when opening a social media account. (**Rijk Rouppe van der Voort**)

3. Staying informed on social media

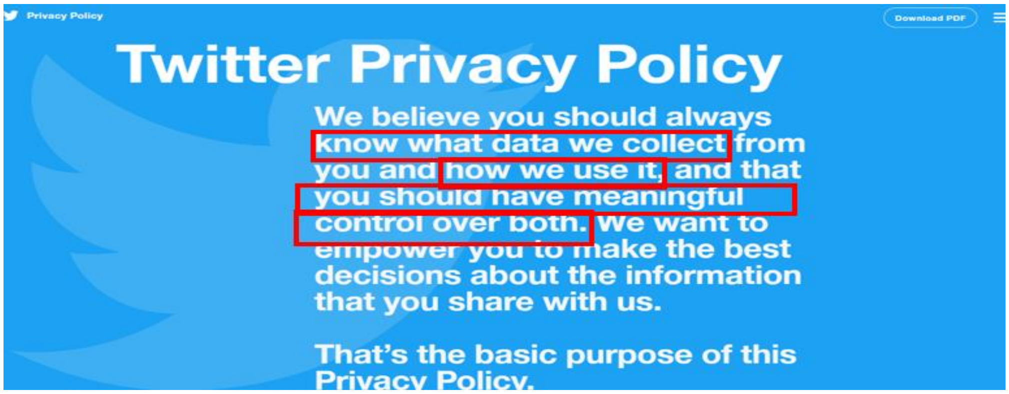
67. Even if the choice of words is not overtly contradictory, problems can arise from the use of ambiguous and vague terms when giving information to users. With such information, users are likely to be left unsure of how data will be processed or how to have some control over the data.

Ambiguous wording. Twitter's Privacy Policy, for example, highlights from the very beginning that users have '*meaningful contro*l' over the data that the Platform collects and how it uses the collected data.[152] However, data subjects must search three long documents in order to gain some control over their data, a procedure proved to be very confusing, intimidating, overwhelming and boring for an average data subject.[153] Thus, the words 'meaningful control' could constitute ambiguous wording aiming to nudge data subjects to believe they are in control, while they are not, in order to share more data than they intended to share (**Quezia Amaral Sayão + Stamatia Beligianni)**

[151] ibid at para 67.

[152] Twitter. (2022). *Twitter Privacy Policy*. https://twitter.com/en/privacy

[153] Schmidt K. (2018). Empowering users to understand their online privacy rights and choices through an interactive social media sign-up process. https://conservancy.umn.edu/bitstream/handle/11299/196363/Empowering%20users%20to%20understand%20their%20online%20privacy%20rights%20and%20choices%20through%20an%20interactive%20social%20media%20sign-up%20process..pdf?sequence=1&isAllowed=y



Twitter Privacy Policy

We believe you should always know what data we collect from you and how we use it, and that you should have meaningful control over both. We want to empower you to make the best decisions about the information that you share with us.

That's the basic purpose of this Privacy Policy.

Screenshot retrieved from <https://twitter.com/en/privacy> accessed 7 April 2022.

69. When online services are offered and addressed to residents of certain Member States, the data protection notices should also be offered in these languages. In this context, it is important that the choice of a particular language can also be switched manually and is implemented continuously without interruptions.

Language discontinuity. The wording of the initial sentence in this paragraph focuses on the residents of a certain Member State, rather than the language in which the website is offered in. Focusing on a more straightforward element, that of the languages offered by the website, would be a better approach, because it would provide better safeguards to the users of the website, namely avoiding language discontinuity, and in making it clear that all privacy-related notices must be offered also in the specific languages in which the website is offered in, rather than focusing on a very specific detail such as the residents of a specific Member State and the language that they speak. This is even more the case with websites also offered in English: with it being a widely known language among EU citizens,[154] would that mean that the service is offered to the residents of all Member States? Or only to those Member States that have a certain threshold of English speakers? Such uncertainties would not be an issue if only the website's languages are considered. **(Antonio Cannavacciuolo + Olga Lampousi)**

While the 2021 Dutch Tiktok case[155] does not specifically mention preference settings, one can assume that the same argument can be made here about providing information in the language spoken by the data subject, particularly when this data subject is a **child.** Therefore, we advise that the guideline emphasizes here that platforms targeted at children be particularly careful at providing preference settings in the language spoken by the data subject. The principle of language continuity in the context of children data subject also relates to recital 58 of the GDPR which states that any processing addressed to a child should be particularly clear and plain and easy to understand, and hence also provided in a language spoken by the data subject. (**Solène Tobler** + **Isabel Sierra Rubio)**

72. 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.

[154] Clark, D. (2019). Share of population with knowledge of English in non-native European countries as of March 2019. https://www.statista.com/statistics/990547/countries-in-europe-for-english/

[155] Autoriteit Persoonsgegevens, 9th April, 2021, *Tiktok* (Accessible online at: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/decision_to_impose_a_fine_on_tiktok.pdf)

Voice interfaces. In relation to specific practices to present settings, **voice interfaces** may also be available to users. These interfaces are suggested by many accessibility guidelines[156] as they can be helpful in increasing understanding of the information provided, especially for users with related disabilities. They can be integrated in smartphones, laptops, sound systems, smart TV and more.[157] Additionally, their usage has rapidly grown with the development of voice assistants, which may be incorporated into many users devices.[158] **(Marina Mijušković)**

82. 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.

DPIA. One recommendation for social media platforms to apply the principles of Data Protection by Design and by Default of Article 25 of the GDPR and to access when data processing is likely to result in a high risk to the rights and freedoms of natural person, is the elaboration of the "**Data protection impact assessment" ("DPIA"**), established by Article 35 of the GDPR. The goal is to help them to identify high risks that could potentially harm data subjects. This assessment procedure can help social media platforms in asking the right questions to ensure they are not engaging in the use of DPs.[159] A risk assessment that could identify potentially DPs for invalid consent can help businesses to prevent them. In addition, the social media providers could even conclude that they might take a risk too high for short term revenue gains in opposite to long term damage to brand reputation, or regulatory fines[160]. The DPIA is required when the data processing is likely to result in a high risk to the rights and freedoms of a natural person and it could be helpful since it includes a proportionality test of the processing compared to its necessity.[161] (**Quezia Amaral Sayão + Stamatia Beligianni**)

4. Staying protected on social media

114. 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.

Social Pyramid dark patterns. The EDPB should include in its guidelines the DPs of '**social pyramid**' which is part of the 'forced action' DPs according to the taxonomy formulated by Gray et al.[162] The 'social

[156] How People with Disabilities Use the Web, W3C – Web Accessibility Initiative WAI - Strategies, standards, resources to make the Web accessible to people with disabilities, availiable on https://www.w3.org/WAI/people-use-web/ .

[157] Mert Aktas, A Definitive Guide to Voice User Interface Design (VUI) UX DESIGN, User Guiding Blog, Decembar 22, 2021, availiable on https://userguiding.com/blog/voice-user-interface/ .

[158] Soofastaei, Ali. "Introductory Chapter: Virtual Assistants". Virtual Assistant, IntechOpen, 2021. 10.5772/intechopen.100248. October 13th, 2021 DOI: 10.5772/intechopen.100248; And M. Vimalkumar, Sujeet Kumar Sharma, Jang Bahadur Singh, Yogesh K. Dwivedi, 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants, Computers in Human Behavior, Volume 120, 2021, 106763, ISSN 0747-5632..

[159] Brook, B. (2021, September 11). *Avoiding DPs: Critical Tools for Privacy Legal Counsel*. CPO Magazine. Retrieved April 5, 2022, from https://www.cpomagazine.com/data-privacy/avoiding-dark-patterns-critical-tools-for-privacy-legal-counsel/

[160] Usercentrics. (2022, February 7). DPs and how they affect consent. Consent Management Platform (CMP) Usercentrics. Retrieved April 14, 2022, from https://usercentrics.com/knowledge-hub/dark-patterns-and-how-they-affect-consent/

[161] Brook, B. (2021, September 11). *Avoiding DPs: Critical Tools for Privacy Legal Counsel*. CPO Magazine. Retrieved April 5, 2022, from https://www.cpomagazine.com/data-privacy/avoiding-dark-patterns-critical-tools-for-privacy-legal-counsel/

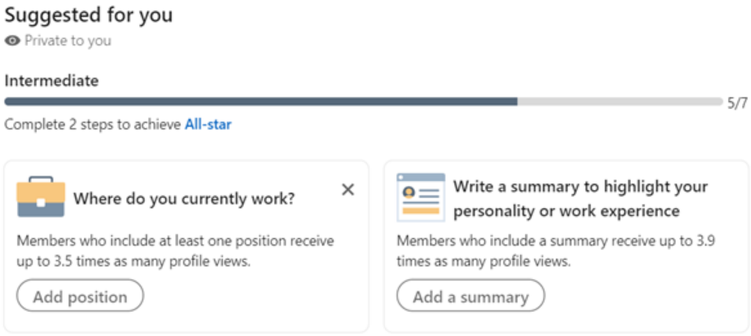
[162] Gray C. M., Kou Y., Battles B., Hoggatt J., and Toombs A. L. (2018). The Dark (Patterns) Side of UX Design. *In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (Montreal QC, Canada) (CHI '18)*. dl.acm.org, 534:1–534:14. https://doi.org/10.1145/3173574.3174108

pyramid' is identified when data subjects are asked and encouraged to recruit others (or allow the social media platform to recruit others on their behalf) to use the platform in return for a benefit and is widely used in social media and gaming platforms.[163] This issue was also tackled by:

- Belgian DPA which investigated the 'invite-a-friend' functionality of a social media provider. The Belgian DPA's held that the processing of personal data of the user's contacts (who were either already members of the platform or non-members) based on such a functionality is unlawful due to the lack of a legal basis --[164]neither Article 6(1)(a) nor Article 6(1)(f) could serve as a lawful legal basis for this functionality.[165]
- Article 29 Working Party has formulated four conditions that must be met cumulatively in order the 'invite-a-friend' functionality to be lawful namely no incentive is given for the sender or recipient, the provider does not select the recipients of the message, the identity of the sending user is mentioned, and the sending user knows the content of the message that will be sent.[166]

Thus, the EDPB should include in its guidelines the 'social pyramid' DPs and analyze the circumstances under which it can be considered a lawful technique. (**Quezia Amaral Sayão + Stamatia Beligianni**)

Progress bars. Some social media platforms use so-called **progress bars to nudge users to 'complete' their profiles by providing more information**. For example, Linkedin displays the progress bar represented in the first Figure, with suggestions on what other information the user should disclose to obtain **the '*All-star'* profile level**. On the one hand, the progress bar might make users feel that they have unfinished tasks making them uncomfortable, and on the other hand, non-financial or social incentives, and rewards, such as Linkedin's different profile levels in the next Figure, have strong effects in motivating users for sharing information.[167] Consequently, this practice might be considered emotional steering.
Secondly, although Linkedin's users can hide some suggestions, as it is shown in the first Figure, but they cannot hide the progress bar until they do not add the suggested data. This might be considered continuous prompting in our opinion because it repeatedly asks Linkedin's users to provide more data, which might end up in providing the asked information after a certain time. Therefore, we highly recommend for the Board take into consideration this practice in the Guidelines. (**Marius Chirtoaca and Patrik Kovács)**



Suggested for you

Private to you

Intermediate

5/7

Complete 2 steps to achieve All-star

Where do you currently work? ✕

Members who include at least one position receive up to 3.5 times as many profile views.

Add position

Write a summary to highlight your personality or work experience

Members who include a summary receive up to 3.9 times as many profile views.

Add a summary

Screenshot – Linkedin's Progress Bar

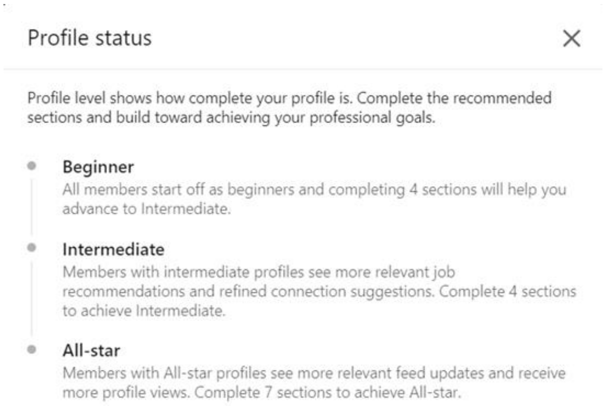
[163] Ibidem

[164] GDPRHUB. (2021, March 31). *APD/GBA - 25/2020.* https://gdprhub.eu/index.php?title=APD/GBA_-_25/2020

[165] Hunton Andrews Kurth. (2020, May 27). *Belgian DPA Sanctions Social Media Company for Unlawful Processing of Personal Data in Connection with "Invite-a-Friend" Function*. Privacy and Information Security Law Blog. https://www.huntonprivacyblog.com/2020/05/27/belgian-dpa-sanctions-social-media-company-for-unlawful-processing-of-personal-data-in-connection-with-invite-a-friend-function/

[166] Article 29 Working Party (2009, June 12) Opinion 5/2009 on social networking. 01189/09/EN WP 163. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

[167] Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2018). Nudges for Privacy and Security. ACM Computing Surveys, 50(3), 1–41. https://doi.org/10.1145/3054926



Profile status

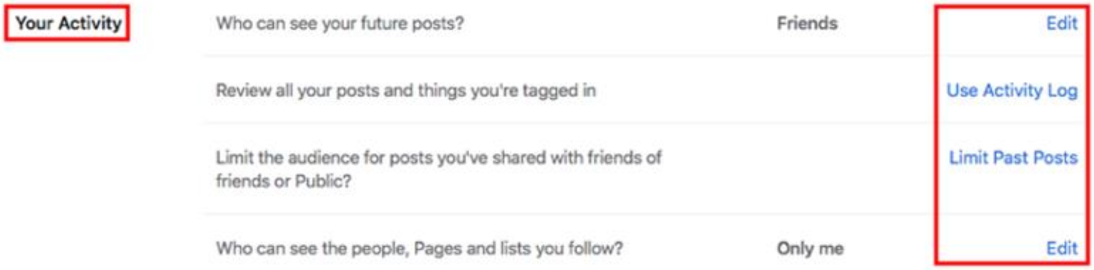
Profile level shows how complete your profile is. Complete the recommended sections and build toward achieving your professional goals.

- **Beginner**
  All members start off as beginners and completing 4 sections will help you advance to Intermediate.
- **Intermediate**
  Members with intermediate profiles see more relevant job recommendations and refined connection suggestions. Complete 4 sections to achieve Intermediate.
- **All-star**
  Members with All-star profiles see more relevant feed updates and receive more profile views. Complete 7 sections to achieve All-star.

Screenshot – Linkedin's Profile Status Levels

Overloading - Too many options
118. 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.

Lack of 'bulk' controls for settings. Making settings related to the same aspect of data protection available in a single and prominent position might still amount to *hindering* if there is a *lack of 'bulk' controls for settings*.[168] Namely, the use of granular controls takes time and effort, which may discourage users from making changes.[169] For instance, to change the visibility of their activity, Facebook requires its users to individually edit each corresponding aspect, such as 'Who can see the people, Pages and lists you follow?'. Since users cannot generally choose the (visible to) 'Only me' option, they may stick with a more privacy-invasive default option, even if it is not their first choice. Therefore, this paragraph of the Guidelines should also state that settings related to the same aspect of data protection should preferably allow being adjusted with a 'bulk' control. Relating this to the example, instead of requiring users to individually edit each aspect of the visibility of their activity, there should also be the possibility to set the visibility to 'Only me' using a 'bulk' control. (**Eva Opsenica + Joanna Taneva**)



Your Activity	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
	Who can see the people, Pages and lists you follow?	Only me	Edit

Screenshot - Lack of a 'bulk' control to edit settings regarding the visibility of the user's activity. Recorded on 1 April 2022, https://www.facebook.com

5. Staying right on social media: Data subject rights

ii. Interface-based patterns
Overloading – Privacy Maze (Annex checklist 4.1.2)

[168] Gunawan, J., et al (2021). A Comparative Study of DPs Across Web and Mobile Modalities. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 1-29, 28. https://doi.org/10.1145/3479521
[169] ibidem

141. 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.

Icons for privacy polices and exercise of rights. To facilitate the readability of privacy policies and the exercise of data subject rights, the Guidelines should also encourage social media providers to use **icons** as per Article 12(7) GDPR – either in combination with a layered privacy policy or not.[170] Since privacy policies contain vast amounts of written information, social media providers could use icons to help users navigate to particular aspects of the privacy policy. **Using icons alongside text may also aid user comprehension of the provided information[171] and overcome communication barriers due to users' different literacy levels**.[172] However, icons' utility is dependent upon their standardisation within the EU; thus, it would be appropriate for the Guidelines to provide an icon set[173] instead of leaving their design to social media providers. In this regard, the Italian DPA recently held a contest for solutions to make information notices simpler, clearer, and immediately understandable through graphic elements, which resulted in icon sets that are now publicly available[174] and freely usable under CC BY 4.0.[175] Accordingly, it might be appropriate to include the first runner-up's icon set in the Guidelines. (**Eva Opsenica + Joanna Taneva**)

Icons for the exercise of rights. Many websites use icons to present information and navigate users in the process of 'singing up' or just staying on the platform. Scholars have been examining icons as a way to provide clear and plain information in order that users understand and knowingly agree.[176] Studies found that some icons are widely familiar and recognisable.[177] For instance, participants rated icons for the right to erasure and right to be informed as "*universal, immediate, instantly recognisable, clear, intuitive, unmistakable*" because they are "*grounded in our culture, codified and common on application software*" Another study developed a set of icons for potentially high-risk activities,[178] and introduced privacy icons set pursuant to art. 13 and 14 GDPR, e.g., withdrawal of consent Art. 13 (2) (c) of the GDPR.[179] The Italian DPA launched a contest for making simple and understandable policies, inter alia, using icons.[180]

[170] Article 29 Data Protection Working Party. (2018). *Guidelines on transparency under Regulation 2016/679* (WP260rev.01), para. 17. https://ec.europa.eu/newsroom/article29/items/622227/en

[171] Habib, H., et al. (2021). Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, *63*, 1-25, 3. https://doi.org/10.1145/3411764.3445387

[172] Rossi, A., & Lenzini, G. (2019). Which Properties Has an Icon? A Critical Discussion on Data Protection Iconography. *International Workshop on Socio-Technical Aspects in Security and* Trust, 211-229, 212. https://link.springer.com/chapter/10.1007/978-3-030-55958-8_12

[173] Article 29 Data Protection Working Party. (2018). *Guidelines on transparency under Regulation 2016/679* (WP260rev.01), para. 52. https://ec.europa.eu/newsroom/article29/items/622227/en

[174] Icon sets by the winners of the contest are available at https://www.gpdp.it/web/guest/temi/informativechiare#2.

[175] Garante per la Protezione dei Dati Personali. (2021, December 15). *"Informative chiare": i vincitori del contest lanciato dal Garante privacy*. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9727383

[176] Christopher F. Mondschein, "Some Iconoclastic Thoughts on the Effectiveness of Simplified Notices and Icons for Informing Individuals as Proposed in Article 12 (1) and (7) GDPR." European Data Protection Law Review, Volume 2 (2016), Issue 4, Page 507 - 520.

[177] Rossi et al. DaPIS: a Data Protection Icon Set to Improve Information Transparency under the GDPR, January 21, 2019. page 38.

[178] Paolo Balboni, Kate Francis, CSR project, Developing a New Dimension of Data Protection as a Corporate Social Responsibility (DPCSR) Mixed methodology research project with Stakeholder involvement, available on https://www.maastrichtuniversity.nl/ecpc/csr-project , accessed on 07.04.2022.

[179] PROGETTO A CURA DI: Maastricht European Centre on Privacy and Cybersecurity (ECPC) Licenza CC BY, available on https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9732643.

[180] "Clearer privacy information thanks to icons? It is possible ", The Guarantor launches a contest appealing to collective creativity., available on https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9561395 , accessed on 07.04.2022.

Therefore, the Guidelines should directly reflect on the usage of the icon to avoid unfamiliar and non-standardised icons and to enhance the readability and transparency of the information provided. **(Marina Mijušković)**

Account needed to exercise a subject access request. We would like to recommend the EDPB to consider including under the overloading DPs the scenario where a data subject wants to create a data access request regulated under article 15 but the controller needs information to identify that subject. This situation has been taken into account under the proposed Guidelines of Art. 15 GDPR "*Issues with establishing the identity of the person making the request*".[181] The channel of communication is already complicated, as it would entail that the user needs to find the proper email address to exercise its right first, and later transfer their personal information for controllers to identify the data subject. What is more, if the controller is not able to identify the data subject who is making the request, for example because the organisation only owns an IP address, the controller could incur in an overloading DPs by requesting more information than the strictly necessary to correctly identify the data owner. It would be interesting if the EDPB considered under these guidelines the situation of identification of data subjects and possible DPs involved. (**Solène Tobler + Isabel Sierra Rubio)**

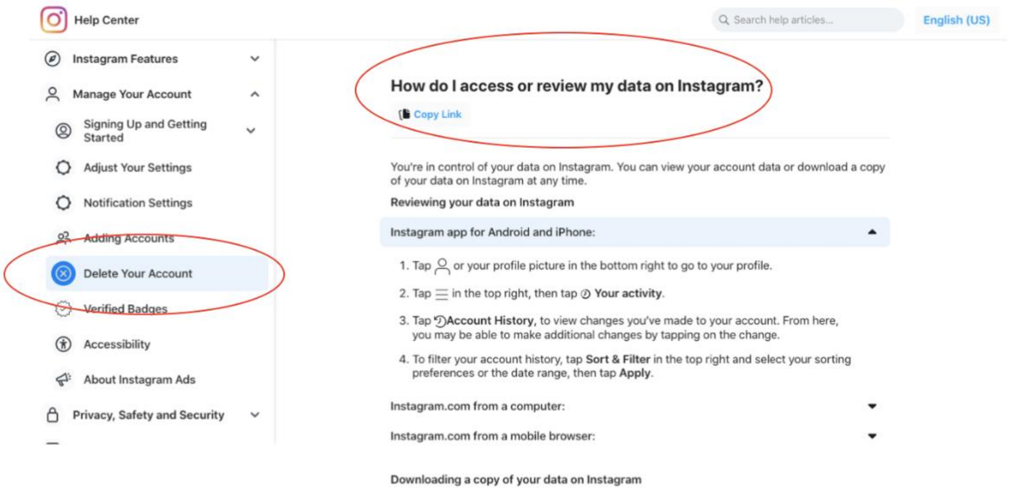
6. So long and farewell: leaving a social media account

Fickle – Lacking Hierarchy (Annex checklist 4.5.2)
Example 49: 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.
146. 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.

Subbject access request and the closing of an account. Regarding data access rights (SAR), social media platforms tend to use a download system tool to create a more automatized way of providing data subjects access to their information.[182] Sometimes, as shown in the screenshot below, interfaces incur in a decontextualizing DPs, in the sense of Article 12.1 regarding easily accessible information, as the download tool may be located under the "delete your account section", which would widely misguide the user. The EDPB could add this part under the **Fickle - Decontextualizing** DPs when getting access rights in social media, as it is unfortunately happening in big platforms, such as the example below. (**Solène Tobler + Isabel Sierra Rubio**)

[181] EDPB Guidelines 01/2022 on Data Subject Rights - Right of Access, 2022, p.23; https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en

[182] Coline Boniface et al. Security Analysis of Subject Access Request Procedures How to authenticate data subjects safely when they request their data. APF 2019 - Annual Privacy Forum, Jun 2019, Rome, Italy. pp.1-20. ffhal-02072302



How do I access or review my data on Instagram?

You're in control of your data on Instagram. You can view your account data or download a copy of your data on Instagram at any time.

Reviewing your data on Instagram

Instagram app for Android and iPhone:

1. Tap or your profile picture in the bottom right to go to your profile.
2. Tap ☰ in the top right, then tap **Your activity**.
3. Tap **Account History**, to view changes you've made to your account. From here, you may be able to make additional changes by tapping on the change.
4. To filter your account history, tap **Sort & Filter** in the top right and select your sorting preferences or the date range, then tap **Apply**.

Instagram.com from a computer:

Instagram.com from a mobile browser:

Downloading a copy of your data on Instagram

153. 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.

Difficult to delete an account. It has been observed that the cases where the users are able to easily create an account, but difficult – or even impossible – to delete it are numerous in practice.[183] More specifically, many times users are obstructed by being required to undertake various steps until their accounts are finally deleted – such as calling during working hours or sending a letter via snail mail.[184] This practice is known as the '*Roacht Motel*', and it infringes the user's need for being subjected to symmetric choices.[185] The *Roacht Motel* DPs is similar to the pattern known as 'Hard to Cancel' which appears to be also restrictive in nature as it limits the ways users can actually cancel their accounts.[186] Recently - as from 31st of January 2022 -, Apple announced an in-app deletion requirement for all the apps apparent in its Store, according to which a mechanism that allows users to delete their accounts from within the apps themselves will be considered as obligatory.[187] We believe that it would be useful for the same requirement to be explicitly introduced in these Guidelines concerning the social media platforms, stating that the users must be able to delete their accounts inside their actual accounts without being forced to proceed to further actions. This could turn the users' interaction with social media platforms into a better experience, reducing the time they spent on this kind of task and, therefore, rendering the users more satisfied. (**Evangelia Cheiladaki + Eleni Arampatzi**)

154. The decision to leave the social media platform triggers not only the consequences of erasure as stated in Article 17 (1) GDPR. Some data remain with the social media platform for a certain period of time if Article 17 (3) GDPR is applicable. However, users' requests to delete their social media account must be understood as implicit withdrawal of consent under Article 7 (3) GDPR.

[183] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. CHI 2018 - Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems: Engage with CHI -Vol. 2018-April). Association for Computing Machinery. https://doi.org/10.1145/3173574.3174108

[184] Luguri, J., Strahilevitz, L., J., (2021). Shining a Light on DPs. Journal of Legal Analysis, Volume 13, Issue 1, 2021, Pages 43–109.

[185] ibid.

[186] Mathur, A., Acar, G. Friedman, J. M., Lucherini, E., Mayer, J., Chetty, M., Narayanan, A. (2019). DPs at Scale: Findings from a Crawl of 11K Shopping Websites. Proc. ACM Hum.-Comput. Interact., Vol. 3, No. CSCW, Article 81.

[187] Julia K. Kadish, (2022). Apple To Require Ability to Delete Accounts In-App. The National Law Review.

Withdrawal and deletion. The deletion of the social media account equals to withdrawal of consent. On the other hand, Article 7 GDPR states that: "the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal." Based on this provision, this article[188] argues that the result of the processing could be preserved. Moreover, it is known that there are machine learning models that end up memorizing all the information used during the processing. Therefore, a definition for the deletion of personal data should be included and a distinction should be made between withdrawal of consent and deletion **(Marius Chirtoaca and Patrik Kovacs)**

> 155. 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 4/2019 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.

Different modalities. A study carried out by Lingareddy et al. found that the deletion process in the case of social media platforms that provide their services through different mediums (mobile applications, mobile browsers, desktop browsers) often differs based on the used medium. Generally, mobile users are more limited to delete their accounts than users who want to do it through a desktop version of the platform: only 7 out of the investigated 20 social media platforms let users to delete their account through their mobile applications, whereas 16 allowed this via a desktop version, and only 4 out of 20 allowed this using any medium.[189] Furthermore, the study also found that some accounts could not be deleted from a desktop browser.[190] In our opinion, these practices do not comply with Article 12(2) of GDPR, because users might be obstructed in the exercise of their right to erasure. Consequently, the Guidelines should emphasise that social media platforms that provide their services through different mediums must allow consumers to delete their accounts via any mediums they are allowed to use. **(Marius Chirtoaca and Patrik Kovács)**

> 158. 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. …

Renewal of consent and the change of a privacy policy. It might be best for the EDPB to establish at the minimum, a practice and a precedent for the durations, at least for social media platforms. It is important that a framework will be built around the duration of consent and a need for consent refresh.
This paragraph mostly reiterates the guidelines on consent by the EDPB from 2020[191], regarding the fact that the GDPR does not specify a time limit in terms of the duration of consent (para 110). Also, the recommendation to refresh at appropriate intervals was mentioned in those guidelines (para 111). A welcome addition to the current guidelines would be to elaborate on what exactly constitutes an "appropriate interval" for each processing purpose, at least when it comes to social media providers.
The main reason why such guidance is necessary is that with the current wording, one possible interpretation a company could use would be that social media platforms could ask the user for consent, even after it has denied consent in the first place, as long as the privacy policy has changed. In the words of the EDPB, "if the processing operations change or evolve considerably, then the original consent is no longer valid". This means that users who had given consent in the first place will have to be asked for their consent again. However, since the privacy policy has changed considerably, users who had initially refused consent might,

[188] Garg, S., Goldwasser, S., &amp; Vasudevan, P. N. (2020, February 25). Formalizing data deletion in the context of the right to be forgotten. arXiv.org. Retrieved April 15, 2022, from https://doi.org/10.48550/arXiv.2002.10635

[189] Lingareddy, N., Schaffner, B., and Chetty, M. Can I Delete My Account?: DPs In Account Deletion On Social Media (2021) CHI 2021 Workshop on What Can CHI Do About DPs?

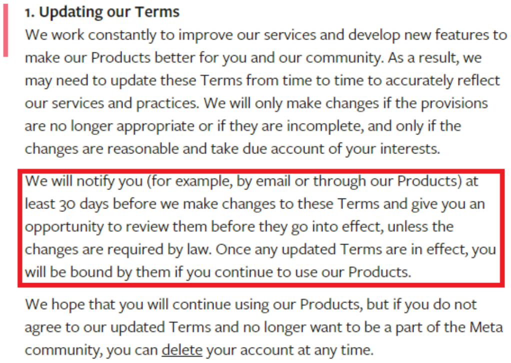
[190] ibidem

[191] European Data Protection Board. (2020, May). *Guidelines 05/2020 on consent under Regulation 2016/679* (1.1). https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

under the new policy, want to give consent anyway. With this interpretation, all users could be asked for their consent every time the policy changed considerably. If this happens often enough, this practice could be a continuous prompting DPs (see paragraph 28). Alternatively, to the EDPB introducing guidance regarding the appropriate interval, it could clarify whether the logic that some DPAs have used regarding tracking cookies consent could be applies to certain data processing by social media providers. For example, the French CNIL have said that the consent duration can be maximum 13 months.[192] In order to prevent situations where following the EDPB's recommendation to refresh consent at certain intervals would lead to DPs like continuous prompting, more guidance regarding consent duration and when to ask for refreshed consent (and to whom) is important. This is especially important because in both case law and academic literature the topic of duration of consent is scarcely available, if at all. (**Tomas Baçe + Arystan Jazin)**

Renewal of consent. Given the rapid changes in Big Data and data analysis, consent is presented in a 'forever' manner and can easily become outdated when the user consent no longer reflects the user preference.[193] Numerous websites, including social media platforms, notify their users on policy changes, but do not necessarily engage the user and request '**renewed' consent,** instead indicating that continued use of the social media service constitutes an acceptance of the amended terms and policies.[194] An example of this practice is the terms of service of *Meta Platforms Ireland Limited* where the user is provided with 30 days to review any changes to the terms. Once the terms come into effect, the user will be bound by the terms without 'consenting' thereto if the user continues to use the service. Considering the above, Custers[195] suggests the inclusion of a provision in the existing legal framework that consent, when not renewed, expires after a period of 2 or 3 years.

- The first rationale for this time frame is that when users are regularly asked to renew their consent, a more engaged user may come to the realization that they have changed their mind, for example because the way in which their personal data is being processed has changed.
- The second rationale may be that a user better understands the consequences of their consent after being a user of a social media platform service for 2 or 3 years when compared to when they first signed up.
- Such approach would not only be beneficial in ensuring that consent is constantly kept up to date but also to reduce the risk of 'function creep', which is when data is used for purposes other than the purpose for which it was initially collected. **(Jasper Hille + Roberto de Alcântara)**



1. Updating our Terms

We work constantly to improve our services and develop new features to make our Products better for you and our community. As a result, we may need to update these Terms from time to time to accurately reflect our services and practices. We will only make changes if the provisions are no longer appropriate or if they are incomplete, and only if the changes are reasonable and take due account of your interests.

We will notify you (for example, by email or through our Products) at least 30 days before we make changes to these Terms and give you an opportunity to review them before they go into effect, unless the changes are required by law. Once any updated Terms are in effect, you will be bound by them if you continue to use our Products.

We hope that you will continue using our Products, but if you do not agree to our updated Terms and no longer want to be a part of the Meta community, you can delete your account at any time.

Screenshot of https://www.facebook.com/terms.php. Emphasis ours. Recorded on 15 April 2022.

[192] Santos, C., Bielova, N., & Matte, C. (2020). Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. *arXiv*, 1–75, p. 35, https://doi.org/10.48550/arXiv.1912.07144

[193] Custers, B. (2016). Click here to consent forever: Expiry dates for informed consent. *Big Data & Society*, *3*(1), 2053951715624935, p.3.

[194] ibid.

[195] ibid.

163. 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.

FOMO and design friction techniques. DPs using emotional steering might exploit the phenomena of **FOMO**[196] and it is '*characterized by the desire to stay continually connected with what others are doing*'.[197] (already identified within the signing in process). In our opinion, the Guidelines should consider the different design friction techniques, such as *microboundaries, slow design, or uncomfortable design,*[198] to provide valuable solutions for reducing the harmful effects of emotional steering, especially in case of Fear of Missing Out.

- *Microboundaries* are small obstacles prior to the interaction to prevent users from rush between different contexts, whereas uncomfortable interactions try to cause deliberate discomfort to the users with the aim of memorable interactions.[199]
- *Slow or uncomfortable design* is a design philosophy which '*encourages people to to do things at the right time and the right speed which helps them to understand and reflect on their actions*'.[200]

In our opinion, the ethical use of these practices might influence the users during the deletion process to slow down and think over their decision to decrease the possibility of exploiting their fears and emotions. However, the Guidelines must find a balance in using these techniques to avoid another DPs referred to in the Guidelines, the *Longer than necessary* pattern. **(Marius Chirtoaca and Patrik Kovács)**

Cancel account and grace period. While exercising the right to erasure, the right to delete social network accounts, most if not all, use the "grace period". It includes a time span during which the user can cancel his account deletion. For example, Facebook extended the "grace period" for permanently deleting user accounts from 14 days to **30 days.**[201] This is their current practice. This poses a serious issue for subscribers who have problems with Social Network Site addiction,[202] especially as Facebook is recognized as" addictive tech".[203] Studies already pointed out that Facebook employs DPs, e.g., deployment of logout button.[204] Thus, this period could be interpreted as the influence on user behavior as users are tempted to reconsider their decision to delete their account. Furthermore, studies on how companies use tactics to steer users from deleting their accounts showed that companies employ many DPs to prevent users from quitting, e.g., staying on the platform because interface makes it feel" right". [205]In relation to that, the screenshot below depicts the deletion request on Facebook, although the use of wording does not confer the information in a highly negative outlook, it does present an emotional burden for some vulnerable groups. Therefore, it would be advisable for the EDPB to identify and include this type of practice in these guidelines.

[196] Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. Computers in Human Behavior, 29(4), 1841–1848. https://doi.org/10.1016/j.chb.2013.02.014

[197] ibidem

[198] ibidem

[199] Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. Computers in Human Behavior, 29(4), 1841–1848. https://doi.org/10.1016/j.chb.2013.02.014

[200] Grosse-Hering, B., Mason, J., Aliakseyeu, D., Bakker, C., & Desmet, P. (2013). Slow design for meaningful interactions. ACM. https://doi.org/10.1145/2470654.2466472

[201] Nick Statt, 'Facebook extends account deletion grace period from 14 to 30 days' (The Verge, 3 October 2018) <www.theverge.com/2018/10/3/17933264/facebook-account-deletion-grace-period-extension-30-days> accessed 13 April 2022

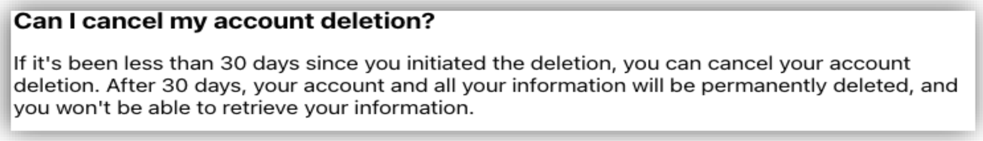
[202] Andreassen, C.S., (2015). Online Social Network Site Addiction: A Comprehensive Review. Curr Addict Rep 2:175–184 DOI 10.1007/s40429-015-0056-9

[203] Kate Raynes-Goldie, DPs: The secret sauce behind addictive tech, January 30, 2020., TechXplore, available on https://techxplore.com/news/2020-01-dark-patterns-secret-sauce-addictive.html

[204] Thomas Mildner, Gian-Luca Savino, How Social Are Social Media The DPs In Facebook's Interface, March 2021, available on https://arxiv.org/abs/2103.10725 .

[205] Runge, J., Wentzel, D., Huh, J.Y. *et al.* "DPs" in online services: a motivating study and agenda for future research. *Mark Lett* (2022). https://doi.org/10.1007/s11002-022-09629-4, page 5.

(**Marina Mijušković + Dušan Stevanović**)



Can I cancel my account deletion?

If it's been less than 30 days since you initiated the deletion, you can cancel your account deletion. After 30 days, your account and all your information will be permanently deleted, and you won't be able to retrieve your information.

Screenshot of Facebook Help Center as of 2022, retrieved from <https://www.facebook.com/help/224562897555674/?helpref=search&query=delete%20account%20permanently&search_session_id=5419a478ba94a48a5b94ac0cfcd7896e&sr=0> accessed 13 April 2022

169. 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.

For the DPs 'hindering', the Guidelines should explicitly mention the 'Dead End' DPs (Annex checklist 4.4.1).

- Lingareddy et al. have found that for the 20 social media platforms they studied, only 5 of them allowed account deletion for each access medium and platform.[206]
- According to a social media consumer study from 2018, most social media users access social media through mobile applications (67%),[207] making it all the more problematic that only 2 of the social media platforms studied by Lingareddy et al. offered account deletion through the mobile application.[208]

This creates a 'Dead End' DPs where it is impossible to delete an account from within the application, and forces a user to access the social media through another platform. It could also be in breach of the GDPR in cases where the application does not allow for deletion, but does allow for the creation of an account, as exercising the right to erasure must be understood as implicit withdrawal of consent under Article 7 (3) GDPR, and 'it shall be as easy to withdraw as it is to give consent'. **(Jasper Hille + Roberto de Alcântara)**

4 ANNEX: LIST OF DPS CATEGORIES AND TYPES

This comment is regarding the layout of the guideline. We believe that it would be more user friendly to add a **table** instead of a list which contains all the various DPs types. This will ensure a better overview of the DPs categories. Perhaps such a table can be added in addition to the current list, however that may cause redundancy. **(Elena + Magdalena)**

[206] Lingareddy, N., Schaffner, B., & Chetty, M. (2021, april). Can I Delete My Account?: DPs In Account Deletion On Social Media. https://drive.google.com/file/d/190uWk2bhJngE0J_K_kGt2v91z_f01Ocz/view, p. 3, 'table 2'.

[207] How People Use Social Media. (2018, 17 oktober). The Manifest. Geraadpleegd op 15 april 2022, van https://themanifest.com/social-media/blog/how-people-use-social-media.

[208] Lingareddy, N., Schaffner, B., & Chetty, M. (2021, april). Can I Delete My Account?: DPs In Account Deletion On Social Media. https://drive.google.com/file/d/190uWk2bhJngE0J_K_kGt2v91z_f01Ocz/view, p. 4.