




Improving the Usability of Requests for Consent to Use Cookies

Kristina Lapin^(✉)  and Laima Volungevičiūtė

Vilnius University, Vilnius, Lithuania
kristina.lapin@mif.vu.lt

Abstract. An HTTP cookie (hereinafter cookie) is a piece of information that maintains a state in a stateless HTTP protocol. Recently established privacy and security regulation imposes an obligation on the service provider to obtain the user's consent to use cookies. This paper is aimed at studying usability guidelines of requests for consent to use cookies (hereinafter consent requests). The consent requests have usability issues that make it difficult for the users to choose the right privacy and security options. A study of privacy and security regulation is aimed at extracting design requirements. Manipulative designs also known as dark patterns are explored and applied to assess consent requests of two of the most popular Lithuanian news portals. An evaluation revealed the presence of dark patterns in consent requests as well as violation of privacy and security requirements. As a result, usability guidelines on the design of cookie consent requests are developed.

Keywords: HTTP cookies · cookie consent requests · dark patterns · security · privacy

1 Introduction

An HTTP cookie is a small piece of information passed between a web server and a browser [1]. This is a collection of information the server creates when a user visits a website [2]. The information stored in the cookies helps the website to identify the user or restore the options set by the user – it can be login, the pages visited by the user on the website, or other usability options, such as language and font size.

Cookies are used to check whether two received requests were sent from the same web browser and to remember the state of the website, for example, stored information about what goods are placed in an e-shop cart. Although the purpose of cookies is to track the state of the web page which would be lost when the user leaves the domain, more detailed purposes are often distinguished [3]: (a) *strictly necessary cookies* for the smooth functioning of the website; (b) *preferences cookies*, such as language, font size, login name, and password; (c) *statistics cookies* collect information about the user's behavior on the website, such as links the user visited; (d) *marketing cookies* track user activity on the Internet to help deliver personalized advertising.

Depending on the collected content, cookies may endanger users' privacy [4]. Users' devices and their information are recognized as personal space in the European Union

(hereinafter EU) law. According to EU law, to process users' personal data, service providers must inform them about the methods of data processing and obtain their consent [5]. Implementing the law, cookie consent requests are introduced on the websites. However, the consent requests require additional mental effort that occurs unexpectedly when opening the page, thus usability issues arise.

The design of consent requests usually does not help the users understand what they are agreeing to. Even more, designers use knowledge of user behavior (e.g., psychology, A/B testing) to generate as many consents as possible when designing consent requests. Such misleading designs are called dark patterns [6]. They are also widely used in social blogs, online stores, mobile apps, and even computer games [7]. Consent requests include various dark patterns, such as information hiding, manipulation of element positions, formatting, blocking of the website content, the abundance of choices, hard-to-see text or links to additional settings, and pre-marked choices [8]. This manipulation degrades the user experience of using the website.

This paper aims to formulate usability guidelines facilitating the design of consent requests that meet privacy and security requirements, are easier to understand, and are less annoying to users. For this purpose, the next chapter explores essential privacy and security requirements. The third section examines dark patterns found in cookie consent requests. Further, the evaluation of consent requests of the most popular Lithuanian news portals based on revealed requirements and dark patterns is conducted. Finally, the usability guidelines facilitating the design of more usable cookie consent requests are formulated.

2 Privacy and Security Regulation

The laws regulating the processing of personal data in the European Union are defined in the General Data Protection Regulation (hereinafter referred to as GDPR). In this regulation, personal data is defined as any information relating to a person whose identity can be or has already been identified [9]. According to the EU directive on privacy and electronic communications supplementing it (hereinafter referred to as E-Privacy Directive) [3], service providers must obtain the user's consent to use cookies that are not necessary for the provision of the service [10]. To obtain consent, service providers use requests on their websites that are accepted when the user first visits the website. To process personal data, service providers have to receive the consent of the person concerned. The GDPR sets out the rules for consent-based data processing, some of which relate to the usability of the consent requests [11]:

- design must ensure that the users understand what they are consenting to;
- consent must be given freely and provided in clear and understandable language;
- consent is not considered freely given if the person does not have a free choice or cannot refuse consent;
- the individual must be able to refuse consent as easily as it is to give it [5, 8].

According to the E-Privacy Directive, cookies may be used provided that users are clearly and accurately informed about the purposes for which they are used [11]. If cookies are not necessary for the functionality provided, such as tracking cookies for

market research, it may be necessary to obtain user consent [12]. Users must be informed about what information is provided to the device they use. The user must also be able to opt-out of cookies when other users have access to personal information stored on the device. Information about the purposes and subsequent uses of cookies must be provided together with information about the user’s right to refuse cookies before they are used. If the user decides to refuse cookies, the service provider must still provide the minimum services – for example, the website with restricted content.

To process user data, at least one of the several conditions for the processing of personal data provided for by EU laws must be met (e.g. obtaining the consent of the individual). If service providers seek to obtain a person’s consent, it should meet certain requirements and recommendations. Table 1 summarizes the requirements and recommendations that consent should be sought.

Table 1. Privacy and security requirements for cookie consent requests

Identifier	Condition	Description
R1	Given free will	Consent must be freely given. The GDPR recommends that consent should not be considered freely given if the individual has no other choice or option to opt-out
R2	Concrete	Consent must be expressed by clear, affirmative action
R3	Informed	The user must be provided with accurate information about the purposes of data processing and future uses in clear and understandable language
R4	Unambiguous	Consent must be expressed for each purpose for which user data will be processed
R5	Clear	Consent requests must be separated from other matters
R6	Continuous	If consent is requested electronically, the request should be clear, and concise and not unnecessarily interrupt the use of the service
R7	Easy disagreeing	Opting out of cookies should be as easy as accepting them
R8	The right to disagree	Information about the user’s right to refuse the use of cookies must be provided together with information about the purposes of using cookies

3 Dark Patterns in Cookies Consent Requests

Harry Brignull defined dark patterns as a carefully crafted user interface to trick users into doing things they might not otherwise do [13]. Dark patterns are increasingly found in different digital platforms such as social blogs and online stores [7] as well as on the official websites of major companies such as Facebook, Amazon, LinkedIn, and Uber [14–16]. One of the dark patterns – “Privacy Zuckering” – was named after the Facebook

founder due to the difficulties of managing privacy on Facebook. Other dark patterns include trick questions, sneak into the basket, Roach motel, price comparison prevention, hidden costs, bait and switch, confirmshaming, disguised ads, forced continuity, and friend spam [15]. Gray et al. categorized Brignull's identified dark patterns into five types: nagging, obstruction, sneaking, interface interference, and forced actions [16]. A study by Luguri and Strahilevitz revealed that the more aggressively dark patterns are applied, the more likely users are to succumb to manipulation and make choices that are against their interests [17]. Even seemingly small design decisions, such as highlighting the consent option or moving the decline button to another window, can significantly increase the likelihood of obtaining user consent [5].

Dark patterns are often observed in cookie consent requests. A study on the top 1,000 EU websites revealed that 57.4% of requests use at least one dark pattern in 2019 [18]. The following design solutions containing dark patterns are met in consent requests [8]:

- *Consent walls* are pop-up windows that contain part of the service provider's privacy policy or informative text about the use of cookies on the website. They clearly separate consent request from other matters, thus satisfying the GDPR requirement (R5). However, consent walls block access to the website until users express their consent. This can be seen as not freely given consent (R1 unsatisfied). Thus, the dark pattern of forced action can be assigned. The dark pattern of nagging is also observed as a consent request is displayed immediately after visiting the website.
- *Tracking walls* are a type of consent walls, in which the user can only accept the use of cookies or leave the site. This design uses the dark pattern of forced action which is more aggressively applied than on consent walls. The tracking wall is a sort of barrier that prevents the user from taking the desired action. Therefore, this design is also a case of the obstruction dark pattern.
- *Reduced service* is provided when the users do not accept the privacy settings. If no alternative is provided to access the full content (for example, a paid service option), the user is forced to agree with the use of cookies to reach the full functionality of the website. This situation can be described by the dark pattern of forced action. Also, redirecting a user to a version of a site with restricted content or functionality could be regarded as nagging.
- *Manipulation of configurations* encourages users to accept the use of cookies. Visual manipulations such as different sizes, position, formatting (use of different colors and fonts), an abundance of options, and pre-marked options aim to make one option more noticeable, and more attractive than the other and secretly encourage the user to choose it. Such manipulation is characterized by the dark pattern of interface interference.

Dark patterns exploit the users' limited attention because they often multitask while browsing the Internet. Designers use attention diversion techniques in request configurations, which draw the user's attention to one part of the website to divert it from other parts that would be more useful to the user [19]. A study conducted by Utz and others shows that such design decisions as moving the position of the request from the top to the bottom of the screen or highlighting the consent button influence the choice of users to express consent or disagreement with the use of cookies. The study observed that

the probability of consent to the use of cookies increased from 0.16% to 83.55% when pre-tagged options were used in the request [18].

4 Evaluation of Consent Requests in Lithuanian News Portals

Evaluation of the design of cookie consent requests was conducted on the two most visited news portals in Lithuania: Delfi.lt and Lrytas.lt [20]. In the assessed requests, consent was expressed using the “I agree” button in the main request window (R2 is met) (see Figs. 1 and 2). However, an option to disagree was not presented in the first window of any request (R7 is violated), therefore disagreement requires more clicks than expressing consent. Each request allows the user to change specific goal settings separately (R4 is met) and the consent request was clearly separated from other questions (R5 is met).

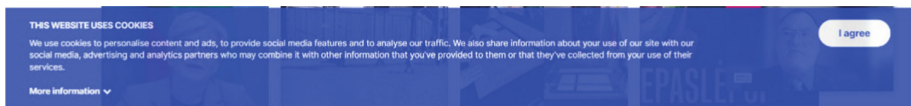


Fig. 1. The first window of cookie consent request on Delfi.lt (<https://www.delfi.lt/en/> – the English version of Delfi.lt)

Delfi.lt consent request is designed in notification bar style and does not interrupt the use of the service (R7 is met). Lrytas.lt uses a consent wall-type request, it is displayed immediately after opening the website which is a case of nagging. However, its sole purpose is to inform the users about the use of cookies and to obtain their consent, so it can be said that it is not an unnecessary interruption (R6 is met).



Fig. 2. The first window of cookie consent request on Lrytas.lt (<https://www.lrytas.lt/english> – the English version of Lrytas.lt). Although the English version is activated, the request is presented in Lithuanian. Below two options are presented: “More options” – on the white button and “I agree” – on the red one.

Although information about the user’s right to disagree was provided only by Lrytas.lt in the first request window, this right was indicated in both examined sites (R8 is met). Lrytas.lt provided an option in the main window that leads to the cookie setting window, so the user can understand that consent is not the only option. In the Delfi.lt

consent request, the cookie settings are hidden under the less visible “More information” dropdown. The user may not even find the hidden settings without carefully examining the request and think that the only option is to accept the setting of cookies (Fig. 3). This raises doubts about whether the consent received is freely given (R1 is violated). The same doubts are raised by Lrytas.lt developers decision to block the site’s content and secretly encourage users’ consent by highlighting the “I agree” button.

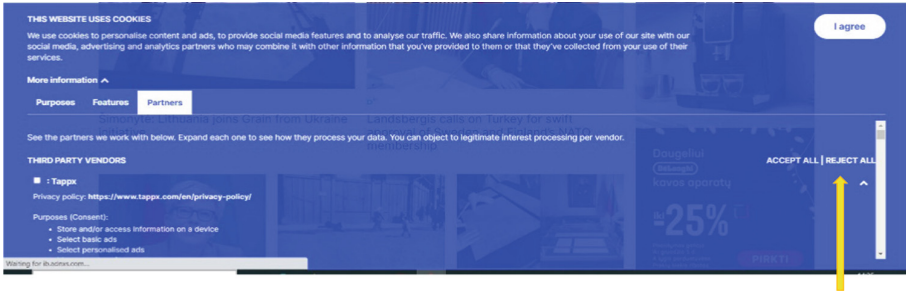


Fig. 3. Expanding “More Information” on Delfi.lt. It is hard to notice that the rejection of all options is available, because of the small text on the right (indicated by a yellow arrow). The user cannot decline individual options.

Lrytas.lt provides the users with detailed information about the data collected and the purposes of processing – for each partner it is indicated what information is collected, the expiration date of the cookie is presented and the goals are clearly stated (R3 is met) (Fig. 4).

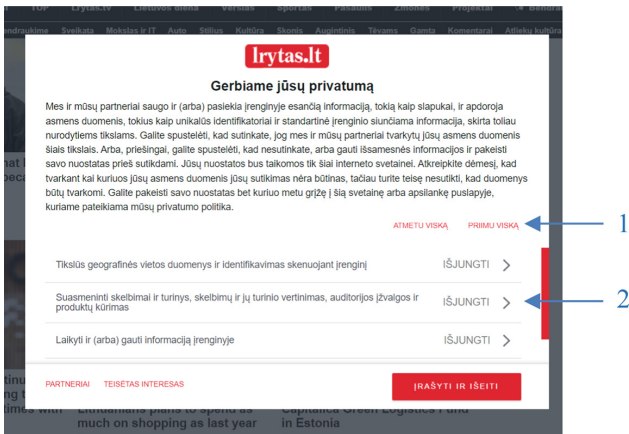


Fig. 4. Presentation of the categories of collected data. Label 1 indicates “Accept all” and “Reject all” options. Label 2 shows an option to decline individual categories. This implicitly means that all options by default are enabled.

Part of Delfi.lt information related to partners is not translated from English, which may not be understandable to all Lithuanian users (R3 is violated).

The four dark pattern categories were found on the assessed sites. Dark patterns of nagging, obstruction, forced action, and interface interference are observed in all sites examined. The obstruction pattern makes it difficult to reject cookies when such an option is not provided in the first request window. The dark pattern of interface interference is observed on Delfi.lt where users are not informed about the user right to disagree with the use of cookies in the first request window. Moreover, Lrytas.lt tries to hide from users that some options are enabled by default. The dark pattern of interface interference manifests itself in the consent option that is presented in all requests more attractively than the option that directs to cookie settings. Delfi.lt used a less noticeable drop-down element for cookie settings. The dark pattern of forced action is observed only at Lrytas.lt in which the content is blocked until the users express their choice.

All in all, both examined consent requests have not complied with at least two privacy and security requirements. Four dark patterns were detected on Lrytas.lt, three – on Delfi.lt.

5 Design Guidelines for Cookie Consent Requests

Revealed violations of privacy and security requirements highlight the need for easily applicable guidelines that would support developers in ensuring the privacy and security of consent requests as well as following the GDPR and avoiding dark patterns. Based on the revealed defects, the guidelines for ensuring privacy and security requirements have been formulated (Table 2).

As an example of applying guidelines, the main page of Delfi.lt cookie consent request is redesigned (Fig. 5) by adding the disagree option (G3). Both options require clicking the button which is a clear affirmative action (G1). The information that the user can refuse to use cookies is shown on the first page (G7).

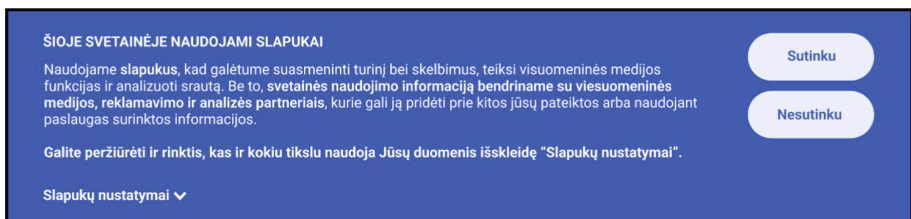


Fig. 5. The redesigned main page of Delfi.lt consent request (in Lithuanian): both options (agree and disagree) are presented as equivalent choices to meet the guidelines G1, G3, and G7.

The example of the application of other guidelines is based on the redesign of the Lrytas.lt site (Fig. 6). Guideline G13 requires facilitating the reading of the lengthy texts. In user interface design this is usually achieved by designing a proper visual hierarchy. Another solution is introducing associative icons. Both solutions are involved in the examined page: icons facilitate quick scanning; the summary of each purpose is

provided in boldface. Further details of each purpose can be obtained by expanding these options. The options to accept or reject all options facilitate the user's decision to refuse more options (G8). Each changeable option indicates its status, whether it is enabled or disabled (G5). More sophisticated design decisions were made to support the quicker perception of texts. A relation between the collected data and their processing purpose (G9, G10) is visualized using graphs and color codes. This solution was popularized by the pribot.org tool for a showing of a privacy policy on Twitter.

Table 2. Usability guidelines for consent requests

Identifier	Description
G1	Consent must be expressed by clear affirmative action, such as clicking a button or checking a checkbox
G2	To ensure that consent is given freely, consent and tracking walls should not be used to obtain consent
G3	Disagreeing with the use of cookies should be as simple as accepting their use. The "Disagree" option has the same importance as the "Agree" option, thus both options must require the same number of mouse clicks
G4	If cookies are used for several purposes, consent should be requested for each purpose separately
G5	If the request uses elements whose state can be changed (e.g., disable/enable, agree/disagree), the setting must have a clear indication of the state (i.e. whether it is enabled/disabled or agreed/disagreed)
G6	The default settings can only be used to activate strictly necessary cookies
G7	The users must be informed about their right to refuse the use of cookies in the first request window
G8	If the consent request requires the user to express an opt-out or objection to more than one legitimate interest, data processing, or partner purpose, an option to facilitate changing the settings of many elements must additionally be provided, such as to reject all listed objectives
G9	The user must be provided with accurate information about the purposes of data processing, data collected, cookies used, and their possible uses in the future, including how cookies can be used and how long they will be valid
G10	If a query contains a lot of information in one place, it should be presented a in visual structure highlighting important points
G11	The user must be informed if the data is shared with third parties
G12	The request must include a link to the website's privacy policy, where the user can find more information about data processing and storage
G13	Getting to know the purposes of data processing should take acceptable time
G14	The design has to ensure that conditions are created for making an informed decision. The elements used in the request must not distract the users' attention or encourage them to make specific decisions
G15	User-relevant information should not be hidden under hard-to-see elements or on additional request pages. If due to the design of the request, it is not possible to present all the information on one page, the request should provide a link where users can find the full text of the information

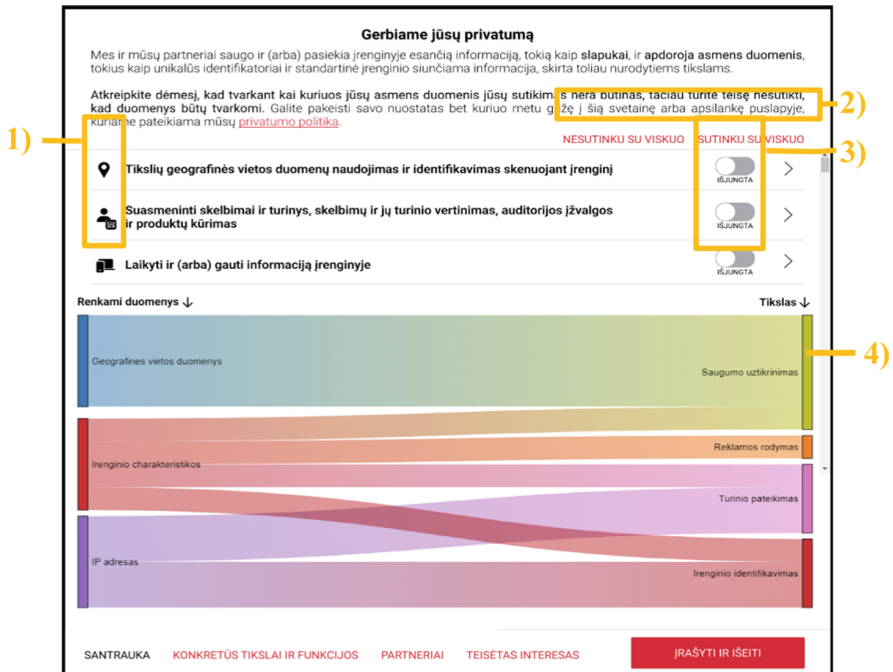


Fig. 6. Redesign of data processing purposes (in Lithuanian): 1) the text of processing purpose is augmented by icons to facilitate quicker content perception (G13); 2) an option to accept or reject all options is provided (G8); 3) all elements whose state can be changed have a clear indication of the state, in the example – disabled (G5); 4) the chart relates the purposes (right edge) with a processed data (left edge), mouseover highlights selected options (G9, G10).

6 Conclusions

This paper aims to establish usability guidelines that would support the usability of consent requests. Recently established regulation for the processing of personal data requires service providers to obtain the user's informed consent to use cookies that are needed for the provision of the service. Implementing this law, each website offers a consent form that contains all the required information. These forms interrupt the current activity and require users to focus on reading a complex legal text. The very fact of the interruption is annoying. The unusable design adds frustration. Therefore, many users decide to minimize the disturbance by choosing the quickest solution that, unsurprisingly, consciously or not, is beneficial for service suppliers. However, unethical behavior will not go unnoticed, thus damaging the users' perception of the provider's brand value. As all sites are required to obtain consent, the sites with more usable solutions will benefit.

The study of GDPR revealed the requirements for ensuring the privacy and security of processing personal user data in web services. These requirements relate usability of consent requests design. Since providers are interested in a specific user choice, the existence of dark patterns in consent requests was checked.

Investigation into dark patterns revealed the presence of four types of dark patterns in the examined consent requests. It was found that the first screen in both examples hides the possibility to reject or choose appropriate cookies on a website. The texts are provided in the form of text walls that hinder their readability. The consent wall prevents the usage of the service until the user will accept with consent request. So, the user's free will is questionable.

Although service providers have an interest to push desirable behavior by accepting all cookies, care for brand value requires considering the users' interests, too. Developed usability guidelines are aimed at facilitating the design of consent requests in future designs. The redesign examples illustrate the usefulness of the developed guidelines. Most of the developed guidelines simply suggest the design decision, such as providing a button that could be clicked or including both options on the first screen. Others are formulated more abstractly. For example, facilitating readability or avoiding distraction. The latter guidelines are subject to further investigation to provide more specific design solutions that would be ready to apply.

References

1. Kristol, D.M.: HTTP Cookies: standards, privacy, and politics. *ACM Trans. Internet Technol.* **1**, 151–198 (2001). <https://doi.org/10.1145/502152.502153>
2. Using HTTP cookies – HTTP—MDN. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>. Accessed 28 Sept 2022
3. Koch, R.: Cookies, the GDPR, and the ePrivacy Directive. <https://gdpr.eu/cookies/>. Accessed 28 Sept 2022
4. Hamed, A., Kaffel-Ben Ayed, H., Kaafar, M.A., Kharraz, A.: Evaluation of third party tracking on the web. In: 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), pp. 471–477 (2013). <https://doi.org/10.1109/ICITST.2013.6750244>
5. Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L.: Dark patterns after the GDPR: scraping consent pop-ups and demonstrating their influence. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1–13. Association for Computing Machinery, New York, NY, USA (2020). <https://doi.org/10.1145/3313831.3376321>
6. Brignull, H.: Bringing Dark Patterns to Light. <https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf>. Accessed 28 Sept 2022
7. Mathur, A., et al.: Dark patterns at scale: findings from a crawl of 11K shopping websites. *Proc. ACM Hum.-Comput. Interact.* **3**, 81:1–81:32 (2019). <https://doi.org/10.1145/3359183>
8. Gray, C.M., Santos, C., Bielova, N., Toth, M., Clifford, D.: Dark patterns and the legal requirements of consent banners: an interaction criticism perspective. *arXiv:2009.10194 [cs]* (2021). <https://doi.org/10.1145/3411764.3445779>
9. Data protection under GDPR. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm. Accessed 28 Sept 2022
10. Santos, C., Bielova, N., Matte, C.: Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. <http://arxiv.org/abs/1912.07144> (2020). <https://doi.org/10.48550/arXiv.1912.07144>
11. General Data Protection Regulation (2016). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=LT>
12. Buthlezi, M.P., Looock, M.: User online privacy and identity management behaviors: a comparative study. In: 2014 Annual Global Online Conference on Information and Computer Technology, pp. 53–57 (2014). <https://doi.org/10.1109/GOCICT.2014.14>

13. Brignull, H.: Dark Patterns: inside the interfaces designed to trick you. <https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you>. Accessed 29 Sept 2022
14. Schlosser, D.: LinkedIn Dark Patterns. <https://medium.com/@danrschlosser/linkedin-dark-patterns-3ae726fe1462>. Accessed 29 Sept 2022
15. Brignull, H.: Dark Patterns. <https://www.darkpatterns.org/index.html>. Accessed 11 Feb 2021
16. Gray, C.M., Kou, Y., Battles, B., Hoggatt, J., Toombs, A.L.: The dark (patterns) side of UX design. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, pp. 1–14. Association for Computing Machinery, New York, NY, USA (2018). <https://doi.org/10.1145/3173574.3174108>
17. Luguri, J., Strahilevitz, L.: Shining a Light on Dark Patterns. Social Science Research Network, Rochester, NY (2019). <https://doi.org/10.2139/ssrn.3431205>
18. Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T.: (Un)informed consent: studying GDPR consent notices in the field. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 973–990. Association for Computing Machinery, New York, NY, USA (2019). <https://doi.org/10.1145/3319535.3354212>
19. Chatellier, R., Delcroix, G., Hary, E., Girard-Chanudet, C.: Shaping choices in the digital world. From dark patterns to data protection: the influence of UX/UI design on user empowerment. Technical report, CNIL (2019)
20. gemiusAudience: September overview of the most popular Lithuanian websites (in Lithuanian). <http://www.gemius.lt/interneto-ziniasklaidos-naujienos/gemiusaudience-rugsejo-mensio-apzvalga-6411.html>. Accessed 12 Oct 2022

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

