




“Your Cookie Disclaimer is Not in Line with the Ideas of the GDPR. Why?”

Anne Hennig¹(✉) , Heike Dietmann¹, Franz Lehr², Miriam Mutter¹,
Melanie Volkamer¹ , and Peter Mayer¹ 

¹ Karlsruhe Institute of Technology, Karlsruhe, Germany
{anne.hennig,heike.dietmann,miriam.mutter,melanie.volkamer,
peter.mayer}@kit.edu

² Technische Universität Dresden, Dresden, Germany
franz.lehr@tu-dresden.de

Abstract. Cookie disclaimers are omnipresent since the GDPR went into effect in 2018. By far not all disclaimers are designed in a way that they are aligned with the ideas of the GDPR, some are even clearly violating the regulation. We wanted to understand how websites justify the use of those cookie disclaimers and what needs to happen for them to change the design of their cookie disclaimers. We, therefore, notified 147 websites (out of the top 500 Alexa German webpages) that their cookie disclaimers are (potentially) not GDPR compliant and asked for their motivation to use specific designs. We also monitored changes at the websites’ cookie disclaimers.

Keywords: Cookie disclaimer · Vulnerability notification · GDPR · EU privacy directive · Web security and privacy

1 Introduction

Since the EU’s General Data Protection Regulation (GDPR) went into effect in 2018, the use of cookie disclaimers got under close scrutiny. If cookies that are not strictly technically necessary are stored or accessed, the EU’s ePrivacy Directive (ePD) requires the consent of the users concerned. The design of the consent mechanism must be in accordance with the provisions of the GDPR.

The authors of [4] examined the cookie disclaimers of the Alexa Top 500 websites in Germany regarding their GDPR compliance. While they identified six categories and various sub-categories of cookie disclaimers, we focused only on two aspects for this study : (1) so-called opt-out procedures which is clearly against the law and (2) highlighting of the *Accept All* option which is nudging users towards accepting all cookies and is legally disputed. Furthermore, we only considered websites that provided the possibility to decline optional cookies. A total of 150 websites of all 500 websites studied in [4] met these characteristics.

The goal of our research was to understand how websites justify the use of non-compliant cookie disclaimers. And – if they indicated that they would not change the current design of their cookie disclaimers – what would need to happen for them, to change the design to a more privacy-friendly one. Understanding the company’s justification processes helps to understand what (still) needs to be done to improve current legislation.

To answer our questions, we contacted the data protection officers of the corresponding websites via email. We developed two types of emails: For those using opt-out procedure, we explained that this is clearly not GDPR compliant and cited corresponding European Court of Justice (ECJ) case law. For those using highlighting, we explained that their cookie disclaimers are not privacy-friendly and might potentially be not GDPR compliant. The design of our email is based on [9]: We used a legal framing and named a researcher from a computer science and a researcher from a legal research group as senders.

We describe related work in Sect. 2. Section 3 gives an overview of the legal background. The study and the results are described in Sect. 4 and 5 respectively. We reflecting on our results and propose directions for future research in Sect. 6. Section 7 concludes our paper.

2 Related Work

There is already quite some research done on how to best inform website operators about security and privacy issues on their websites. While some details are still unclear, it is evident that notifying a website operator about the problem increases remediation rates compared to not notifying them [2, 5, 10, 11, 14, 15]. Besides technical factors like reaching out to a valid email address or passing spam filters by either the mail provider or the company itself, raising awareness is an important parameter for a successful notification campaign [10]. Awareness can be raised by getting the recipient to trust the message and by motivating the recipient to consider the reported misconfiguration as serious [10].

Maass et al. [9] found that trust in notifications can be established by a variety of formal and content-related factors. The authors asked 460 website operators, which previously had received a notification about a GDPR-compliance misconfiguration, in an online survey whether they agree that the type of notification they received made a trustworthy impression. Participants were then asked to determine factors that led them to trust or distrust the messages. The answers were grouped into three categories:

- **Formal aspects:** The right choice of the sender seems to be a huge trust-promoting factor. The authors did not specify which aspects of the sender the participants deemed trustworthy, but hinted at further trust-promoting aspects like providing a logo, letterhead or signature. Furthermore, correct spelling was deemed trust-promoting.
- **Content-related aspects:** The participants named an accurate and detailed description of the problem as well as a clear motivation that is not attached to financial demands of the sender as trust-promoting factors.

- **Verifiability aspects:** Further trust-promoting factors are providing possibilities to verify the sender, for example by providing contact information or - if applicable - providing the possibility to verify the problem. As stated in [3], verification possibilities are the most important factors.

The right framing of the message can have a large impact on the effectiveness of a notification as well. Especially providing external incentives can drive remediation rates [3]. Incentives can be of technical nature, for example when search engines stop referring traffic to compromised websites [12] or browsers flag warnings on websites [13]. Providing legal incentives is also suggested as a possible solution. Letters sent out by a university law group with a framing that imposes possible legal consequences if the misconfiguration is not solved, showed the highest remediation rates in a notification experiment by [9]. In the following study we adapted both the study design and the design of a vulnerability notification from [9].

3 Background

Our focus is on two aspects of cookie disclaimers, which are *opt-out* and *highlighting*. In the following, we define both aspects according to [4].

Cookie disclaimers are defined as using *opt-out* when users have to actively deselect optional cookies. For example, when a check-box is shown, where at least one more checkbox than *only technically necessary cookies* is pre-selected. If the user wants to allow as few cookies as possible, the pre-selected check-boxes have to be deactivated, to allow only technically necessary cookies.

Highlighting occurs when the *Accept all* button is highlighted or emphasized compared to the other button(s), for example, the *Decline* or *Preferences* buttons. *Highlighting* also applies when only the *Accept all* option is visible as a button and the options to decline are integrated in the disclaimer text.

According to the ECJ’s “Planet49” decision (judgment of 1.10.2019 - C-673/17), consent to the setting of cookies is not effective if this was given using an opt-out design, i.e. via pre-selected buttons. Pre-selecting cookies other than technically necessary cookies forces the user to actively deactivate unwanted tracking and is, therefore, not GDPR compliant. In addition, according to the “Orange Romania” decision of the ECJ (judgment of 11.11.2020 - C-61/19), the free decision of users is disproportionately constrained if the refusal of consent represents a greater effort than the granting of consent.

Highlighting heavily nudges users to accept all cookies. The compliance of such designs with the GDPR is disputed. There are first judgments that require an equivalent design of buttons for an effective consent as well as corresponding assessments of data protection authorities that require an equivalent communication effect of presented options. Therefore, it can be interpreted, that a cookie disclaimer violates the GDPR when the option to allow only technically necessary cookies is not equivalent in design to the *Accept all* button. As there is no final judgment, we consider *Highlighting* as potentially not GDPR compliant.

In this paper, we name cookie disclaimers that use only highlighting but no opt-out *Highlighted Only*. All cookie disclaimers that use highlighting and the opt-out procedure are called *Highlighted and Opt-Out Procedure*. Krisam et al. [4] found no website that used an opt-out procedure without highlighting the *Accept all* option. So, we did not consider this for our research either.

4 Methodology

4.1 Design Decisions for Communication

Our methodological design is mainly based on the findings of [9]. For our communication, we also chose a privacy issue that can be tied to a GDPR violation, i.e. privacy-intrusive cookie disclaimers. Note, we talk in the following paragraphs about notifications as this is the common term in the related work – while we do not only notify our recipients about our findings with their cookie disclaimer, but also invited them to answer our questions.

Recipient and Communication Channel. As described in [8], it is necessary to find the appropriate responsible party for a notification on security or privacy issues. In this study, we defined the data protection officers as the responsible party for our notification. Therefore, we gathered the contact information of the data protection officers for the websites in our sample. We considered sending emails as the most practical way for the amount of websites. Correspondingly, we searched for the email address of the data protection officer, but considered universal email addresses of the company (e.g. info@domain.de), contact forms on the websites and postal addresses as possible alternatives. We manually searched for this information in the imprint or on the websites of the corresponding websites. For the *Highlighted Only* - group we collected 123 email addresses (114 of these were from data protection officers and the remaining addresses were general ones), 12 online contact forms and three postal addresses. In the *Highlighted and Opt-Out Procedure* - group we found 11 email addresses (9 from data protection officers), one online contact form and no postal address.

Sender of the Notification. Maass et al. [9] suggest, that legal experts as senders increase the likelihood that the notification is considered serious enough to react on it. Therefore, the notification mentions that this email is sent as part of a cooperation between a computer science and legal research group. A researcher of both groups 'signed' the email (signing in terms of were mentioned as sender). The email as such was sent from the member of the computer science group.

Content of the Notification. We designed our notifications according to the best practices for vulnerability notifications as described in [3, 8, 9]. We used good use of language with respect to correct spelling; we provided a clear motivation and a detailed description of the problem; we provided contact possibilities via telephone and email; and we used a proper signature.

Each email included a short text to provide some information about the research project in general. Then we explained our motivation. Explaining the motivation for a notification and providing detailed information on the problem is considered as a major trust-promoting factor [3]. Since the legal framing turned out to be most effective in [9], our notifications had a legal framing as well. Both groups received the legal information on highlighting, while the *Highlighting and Opt-out Procedure* group received additional information on the opt-out procedure. We referred to the court decisions described in Sect. 3.

Furthermore, we asked the recipients to answer some questions within the next four weeks. We ensured that the answers are analyzed anonymously. We provided the researchers' contact information, in case of questions, and to give the recipients the possibility to verify our notification, as suggested in [3].

Survey Questions. To provide a low threshold for the responses, we included our questions at the end of our email. We used mainly closed-ended questions, and participants could add comments, if wanted. We asked why they used highlighting and (if applicable) opt-out procedures (questions 1 and 2). Possible answers were "not intended", "taken over by default", "intended" or "Other" – while in the last case, they were asked to name the reason. Afterwards, we asked, if they were previously informed about the issue with their cookie disclaimer (question 3). Possible answers were "yes, I was informed", "I was just informed about...", "No, I was not informed" or "Other" – while in the last case, they were asked to describe the situation. Then, we asked whether the data protection officers were involved in the development process of the cookie disclaimer (question 4). Possible answers were "Yes, I was involved as data protection officer", "No, I was not involved" or "Other". Question 5 was an open-ended question, where participants were asked to explain the motivation why highlighting (or highlighting and an opt-out procedure) was applied. Finally, we asked for the future plans (question 6), i.e. whether they are planning to change the cookie disclaimers. Email texts and survey questions are available at [redacted for anonymous review].

4.2 Procedure

An overview of the study procedure is provided in Fig. 1. We considered two groups of cookie disclaimers from Krisam et al. [4]. The first group, *Highlighted Only*, includes 138 websites from the sample considered in [4]. The second group, *Highlighted and Opt-Out Procedure*, includes 12 websites. There were no websites which used the opt-out procedure but did not highlight the accept-all option.

Notifications were sent as an email or via the online contact form in June 2021 with a request for response within four weeks. We excluded the three postal addresses, as we considered it too difficult to guarantee the same level of anonymity for their answers. Consistent with [8], data protection officers managing several websites were only contacted once for all the websites they are in charge of.

Thus, in total, 147 of the 150 websites that showed *Highlighted Only* or *Highlighted and Opt-Out Procedure* were notified. Before sending out the notifications,

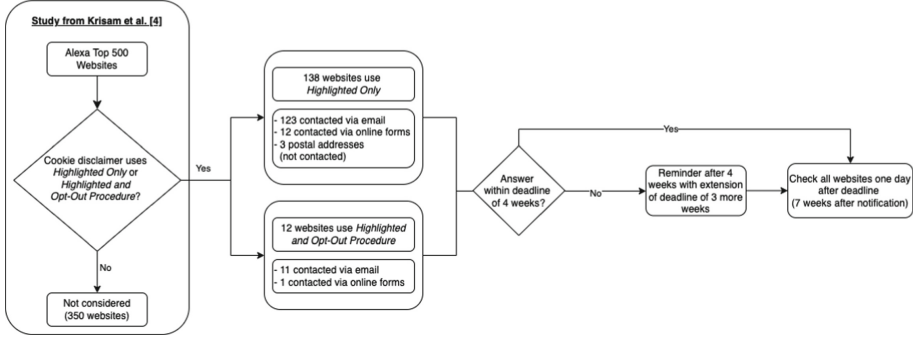


Fig. 1. Description of the methodology

the cookie disclaimers of all 150 websites were analyzed again to make sure they were still in the same category.

Just before the end of the deadline of four weeks, we contacted the contact persons of the websites again in July 2021. We did not put further pressure on the recipients, but rather offered that the deadline could be extended for 3 more weeks, if needed. One day after the end of the extended deadline, all notified websites were manually visited again in private mode to check whether the websites had changed their cookie disclaimers with regard to highlighting. And for the 12 which used opt-out procedures whether they still do so.

5 Results

Table 1 shows the responses to our notification of both groups (*Highlighted Only* and *Highlighted and Opt-Out Procedure*) as well as the number of websites which changed their cookie disclaimers after our notification.

16 contacted persons wrote that they refuse to answer. Five said they will forward the email to the person in charge, but in the end no one answered. Only from seven of 147 contacted websites we received responses to our questions, although some only partial: Only one person answered all survey questions. They noted that the highlighting was not intended and that they were notified about this before. They were not involved in the design process and they wrote that the reasons for the highlighting were unknown to them. They further answered that it is planned to change the current design of the cookie disclaimer and explained the changes the company is going to make. One person answered that their company is currently re-designing the cookie disclaimer and modifications “in several directions” are planned. One person just answered that they were informed about the design process but did not answer any of the other questions. One person said, they cannot tell anything about the process how the cookie disclaimer was created, “because we have no influence on the visual presentation [of the cookie disclaimer]”. One person wrote that highlighting and using an opt-out procedure is intended and that they were involved in the design process.

They did not answer the question whether there are plans to change the current design in the future. But they explained that the current design was created with the help of the state data protection authority and is, therefore, compliant with current regulations. Two others also defended their company’s decisions and stated that the design was used on purpose: While the current design is not unlawful, it, instead, allows the companies to collect valuable user data.

Table 1. Responses to our notifications in the *Highlighted Only* and *Highlighted and Opt-Out Procedure* groups and results of the comparisons of the cookie disclaimers

	Highlighted only		Highlighted and Opt-Out procedure	
	Emails (n = 123)	Online-forms (n = 12)	Emails (n = 11)	Online-forms (n = 1)
Responses with (partial) answers to the questions	6	0	1	0
Emails of refusal	13	3	0	0
Websites that eliminated highlighting and the opt-out procedure after notification	5	0	2	0

One day after the extended deadline ended in August 2021, we visited all 147 notified websites again and took screenshots of their cookie disclaimer. Then we compared those screenshots to the ones we took before we sent out the notifications. We only considered cookie disclaimers to have changed, if they either changed the highlighting and made *accept all* and *deny* buttons similar in design; or if they used an opt-in procedure instead of the opt-out procedure.

We could observe that of the 12 websites notified for using both, highlighting and the opt-out procedure, seven websites changed their cookie disclaimer. Five of those seven websites did not use the opt-out procedure anymore, but kept the highlighting. And two websites changed both, the highlighting and the opt-out procedure. Of the 135 notified websites that only used highlighting to emphasize the *Accept All* button, five websites changed their cookie disclaimers and made both the *Accept All* and the *Deny All* button equivalent in design.

In total, only seven of 147 websites changed the design of their cookie disclaimers to a more privacy friendly option and eliminated both: highlighting **and** the opt-out procedure. Furthermore, we could also observe quite the opposite: Three websites who used *Highlighted Only* before, now used the *Highlighted and Opt-Out Procedure* and, therefore, got even less privacy friendly.

We could also observe that our notification were only partially successful: From the three websites where the cookie disclaimers got less privacy friendly after our notification, two answered our email, but refused to answer our questions. And one did not answer at all. From the seven websites that got more privacy friendly, two websites (partially) answered our questions (one website was from the *Highlighted and Opt-Out Procedure* group, one was from the *Highlighted Only* group). One answered that the email will be forwarded, but no one

got in contact with us afterwards. One website only sent an auto-reply. Furthermore, five websites answered our questions at least partially, but did not change the design of their cookie disclaimers.

6 Discussion

We notified 147 websites – 135 using *Highlighted Only* and 12 using *Highlighted and Opt-Out Procedure* – about the (potential) GDPR non-compliance of their cookie disclaimers and asked for their motivations to use such a design. Yet, we only got very few reactions from the recipients of our notifications (response rate to our questions was 4.67%) and the majority of websites did not change their cookie disclaimers towards a more compliant one.

A possible explanation for the little feedback is that the data protection officers might have not received our notification or the email was considered as spam, as this is a common problem with vulnerability notifications [3]. It is also likely that company’s are not willing to share information on privacy and security issues. Response rates in studies with similar topics were low as well [1, 6, 9, 10, 14]. According to [7], sending letters could increase response rates. However, sending e-mails is still the most (cost-) efficient way for large-scale notification campaigns [10]. Also, we could have asked for answers via alternative channels, like phone. This had been proven successful in [3, 10]. Unfortunately, most of the websites did not provide contact information other than email for their data protection officers. Due to our limited resources, we discarded this option.

We also decided against a framing with tougher legal incentives – a solution that has been suggested in [8]. We explicitly stated the legal problems with the current designs and did not feel responsible for pressing further legal charges. Additionally, expressing legal consequences would have even more diminished our chances to receive answers to our survey questions.

Since we considered the most visited websites in Germany, it is likely that we addressed comparatively big companies. Those companies actually benefit monetarily from the data collected through the cookies, and, furthermore, probably have a team of people handling various data protection topics. According to the careful answers we received, it is likely that the companies we contacted applied a risk-benefit analyses. With the result that the current design of the cookie disclaimers provides low risk of legal consequences, while it increases the likelihood to collect valuable data. This might be one reason for the low compliance rate.

Another reason might be that many websites, including governmental websites, highlight the *Accept all* option in their cookie disclaimers. Also, some websites might use pre-designed templates for their cookie disclaimers where the *Accept all* options are highlighted. Thus, data protection officers and/or chief information officers in companies may come to the conclusion that their cookie disclaimer in place is legally admissible.

It should also be admitted that a data protection officer has to ensure legally compliant data collection, rather than protecting users’ privacy. Furthermore,

data protection officers might not be used and/or entitled to answer surveys. Thus, future studies should reach out to the management level instead.

After we conducted our study, the conference of German data protection supervisory authorities published guidelines that clarified the requirements for legally compliant usage of cookies, including the design of cookie disclaimers, in December 2021. The guidelines confirmed the need for opt-in procedures as well as for equally designed decline options. Although not binding, the guidelines may have affected the design choices of website operators.

Therefore, we checked the cookie disclaimers of all 150 websites again in March 2022 to find out if the new regulations had any effect. We found that 130 of 147 websites still use highlighting. Compared to August 2021, where 140 websites still used highlighting, 10 additional website changed the design and made both options equal in design. Within the *Highlighted and Opt-Out Procedure* group, one website did neither use highlighting, nor the opt-out procedure anymore. Another website discarded only the opt-out procedure. Thus, from 130 websites which use highlighting in March 2022, only six websites still use highlighting *and* opt-out procedure, compared to eight websites which used both in August 2021.

We could also observe that some companies are modifying their cookie disclaimers over time – potentially to find those designs that increase the consent rates without violating current regulations. Still, further research is needed to get a real understanding how websites justify the use of non-compliant cookie disclaimers. With our study we provided possible improvements.

7 Conclusion

With the EU’s General Data Protection Regulation (GDPR) being in effect since 2018, more and more privacy invasive techniques on the web had to be disabled. But the legal situation regarding cookie disclaimers is still a legal gray area.

The goal of our research was to understand how websites justify the design of their cookie disclaimers that either use (1) opt-out procedures which is against the law or (2) highlighting, which is at least against the idea of the GDPR, as one could argue that highlighting is nudging users towards accepting all cookies.

We notified 147 German websites of the Alexa Top 500 that used either *Highlighted Only* or *Highlighted and Opt-Out Procedure* (cf. Sect. 3), that their cookie disclaimers are (potentially) violating the GDPR. Furthermore, we included a short survey to find out how the websites justify the current design and what would need to happen for them to change the design to a more privacy-friendly one. Unfortunately, we got little feedback.

After our reminder deadline ended, 142 websites still used highlighting and 8 of those 142 also used the opt-out procedure. In the end, only seven websites got less privacy intrusive. We checked all cookie disclaimers again in March 2022 and found that 130 websites still used highlighting in their cookie disclaimers, while six of those 130 also used an opt-out procedure. Thus, in the end, 17 out of 147 websites chose for a more privacy friendly design of their cookie-disclaimers.

One possible reason is that the websites weighted the risks for potential penalties – which are rather low, considering the controversial legal situation – against the benefits they have from collecting valuable user data.

Thus, further clarifying case law and a clear positioning of the supervisory authorities is needed to provide unambiguous guidelines for website operators. The recent guidelines on dark patterns in social media platform interfaces by the European Data Protection Board are a step in the right direction.

Acknowledgement. This research is supported by the German Ministry of Education and Research (BMBF), as part of the INSPECTION project (Zuwendungsnummer 16KIS1113), and the Helmholtz Association (HGF) through the subtopic Engineering Secure Systems (ESS). The project was funded by the ministry of Science, Research and the Arts Baden-Württemberg as part of the DIGILOG@BW joint research project with funds from the digilog@bw State Digitization Strategy.

References

1. Ahrend, J.M., Jirotko, M., Jones, K.: On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge. In: CyberSA (2016)
2. Durumeric, Z., et al.: The matter of heartbleed. In: IMC 2014 (2014)
3. Hennig, A., Neusser, F., Pawelek, A., Herrmann, D., Mayer, P.: Standing out among the daily spam: how to catch website owners attention by means of vulnerability notifications. In: CHI 2022 (2022)
4. Krisam, C., Dietmann, H., Volkamer, M., Kulyk, O.: Dark patterns in the wild: review of cookie disclaimer designs on top 500 German websites. In: EuroUSEC 2021 (2021)
5. Kührer, M., Hupperich, T., Rossow, C., Holz, T.: Exit from hell? Reducing the impact of amplification DDoS attacks. In: USENIX Security 2014 (2014)
6. Li, F., et al.: You’ve got vulnerability: exploring effective vulnerability notifications. In: USENIX Security 2016 (2016)
7. Maass, M., Clement, M.P., Hollick, M.: Snail mail beats email any day: on effective operator security notifications in the internet. In: ARES 2021 (2021)
8. Maaß, M., Pridöhl, H., Herrmann, D., Hollick, M.: Best practices for notification studies for security and privacy issues on the internet. In: ARES 2021 (2021)
9. Maass, M., et al.: Effective notification campaigns on the web: a matter of trust framing and support. In: USENIX Security 2021 (2021)
10. Stock, B., Pellegrino, G., Li, F., Backes, M., Rossow, C.: Didn’t you hear me? - towards more successful web vulnerability notifications. In: NDSS 2018 (2018)
11. Stock, B., Pellegrino, G., Rossow, C., Johns, M., Backes, M.: Hey, you have a problem: on the feasibility of large-scale web vulnerability notification. In: USENIX Security 2016 (2016)
12. Vasek, M., Moore, T.: Do malware reports expedite cleanup? An experimental study. In: CSET 2012 (2012)
13. Zeng, E., Li, F., Stark, E., Felt, A.P., Tabriz, P.: Fixing HTTPS misconfigurations at scale: an experiment with security notifications. In: WEIS 2019 (2019)
14. Çetin, F.O., Ganan, C.H., Korczynski, M.T., Eeten, M.J.G.V.: Make notifications great again: learning how to notify in the age of large-scale vulnerability scanning. In: WEIS 2017 (2017)
15. Çetin, O., Jhaveri, M.H., Gañán, C., Eeten, M.V., Moore, T.: Understanding the role of sender reputation in abuse reporting and cleanup. *J. Cybersecur.* **2**, 83–98 (2016)