Global Privacy Enforcement Network

# GPEN Sweep 2024:

# “Deceptive Design Patterns”

Report

July 9, 2024

# Table of contents

## Background

The 2024 Global Privacy Enforcement Network (GPEN) Sweep ("the Sweep") took place during the week of January 29-February 2. It examined the frequency and types of Deceptive Design Patterns ("DDPs") (aka "dark patterns") observed in interactions with websites and mobile applications.

Generally, DDPs are design choices found in platform interfaces that are used to influence, manipulate, or coerce users to make decisions that are not in their best interests.[1] With respect to privacy, DDPs can:

1. Influence users to provide more personal information than is necessary for obtaining products or services;
2. Require users to take extra steps to choose the most privacy-protective option(s); and/or
3. Obstruct users' efforts to obtain privacy-related information.

DDPs can be used either on their own or in conjunction with one another. When two or more DDPs are used together, they can become more effective at influencing users' privacy decisions. The use of one DDP may also facilitate downstream uses of other DDPs.

As individuals spend significant time using websites and apps to perform daily activities, regulatory authorities have become increasingly focused on how those platforms are designed to steer individuals' interactions in a manner that will result in collection of more personal information. For example, the Organisation for Economic Co-operation and Development (OECD), the European Data Protection Board (EDPB), the US Federal Trade Commission (FTC), and the UK Digital Regulation Cooperation Forum (DRCF) have all recently issued separate reports on DDPs.[2]

This year, 26 privacy enforcement authorities ("PEAs") participated in the Sweep, examining 1,010 websites and apps.[3] Owing to the relevance of DDPs to both privacy and consumer protection, for the first time, GPEN conducted the Sweep in coordination with the International Consumer Protection and Enforcement Network (ICPEN), with each network's members looking at DDPs from their respective regulatory angle.

---

[1] "Dark Commercial Patterns," OECD Digital Economy Papers, October 2022, No. 336; European Data Protection Board , "Guidelines 3/2022 on deceptive design patterns in social media platform interfaces: How to recognise and avoid them," version 2.0, Adopted on 14 February 2023.

[2] Ibid.; "Bring Dark Patterns to Light," Federal Trade Commission, Staff Report, September 2022; "Harmful Design in Digital Markets: How Online Choice Architecture Practices can Undermine Consumer Choice and Control over Personal Information," A joint position paper by the Information Commissioner's Office and the Competition and Markets Authority, August 2023.

[3] Specifically, participating PEAs reviewed 899 websites and 111 apps, noting that they may have independently examined different versions of websites and/or apps, such that the number of distinct websites and apps swept may be less than 1,010.

GPEN and ICPEN have collaborated previously, such as on the issuance of a joint news release concerning the Google Play Store, and the organization of a joint enforcement capacity-building workshop in 2021.[4] However, with a total number of 53 participating authorities (26 PEAs and 27 ICPEN authorities), this year's Sweep represents the most extensive example of cross-regulatory cooperation between privacy and consumer protection authorities, to date. This expanding cooperation between GPEN and ICPEN is in recognition of the increasing intersection of the two regulatory spheres in the digital economy.

## Methodology

The goal of the Sweep was for participants, or "sweepers," to replicate the consumer experience by engaging with websites and/or mobile apps to assess how they could (i) make privacy choices, (ii) obtain privacy information, and (iii) log out of and delete an account.

The Office of the Privacy Commissioner of Canada (this year's "Sweep Coordinator") coordinated the Sweep and developed, in collaboration with participating PEAs, a set of instructions and associated questions to guide sweepers' engagement with each website and mobile app. This approach was intended to help identify DDPs, while ensuring that sweepers evaluated websites and apps according to similar standards. The questions focused on five indicators that were based on the taxonomy of DDPs identified by the OECD, and that were considered relevant to both privacy and consumer protection. The indicators, which will be further explained in the relevant sections below, were:

1. Complex and confusing language (i.e., technical and/or excessively long privacy policies that are difficult to understand);
2. Interface interference (i.e., design elements that can influence users' perception and understanding of their privacy options);
3. Nagging (i.e., repeated prompts for users to take specific actions that may undermine their privacy interests);
4. Obstruction (i.e., the insertion of unnecessary, additional steps between users and their privacy-related goals); and
5. Forced action (i.e., requiring or tricking users into providing more personal information to access a service than is necessary to provide that service).

Sweepers were asked to document their observations and interactions with privacy settings, privacy policies, account creation, log out and deletion processes for different websites and apps using the provided questionnaire.[5]

---

[4] "Google Play Store to require app providers to provide consumers with detailed information regarding data collection and use following growing international pressure," ICPEN & GPEN, May 2021.

[5] Because the Sweep was based on the observations and interactions of sweepers with websites and apps, it does not account for deceptive design practices that are integrated into the system architecture (e.g., algorithmic practices that steer users, sometimes subconsciously, toward undesirable choices).

Each participating PEA selected the focus of their Sweep - for example, to examine websites and/or apps in specific industries that aligned with their strategic priorities. As a result, PEAs completed aspects of the questionnaire that were relevant to their Sweep.

The following (Figure 1) is a sectoral breakdown of the websites and mobile apps examined in the Sweep:[6]

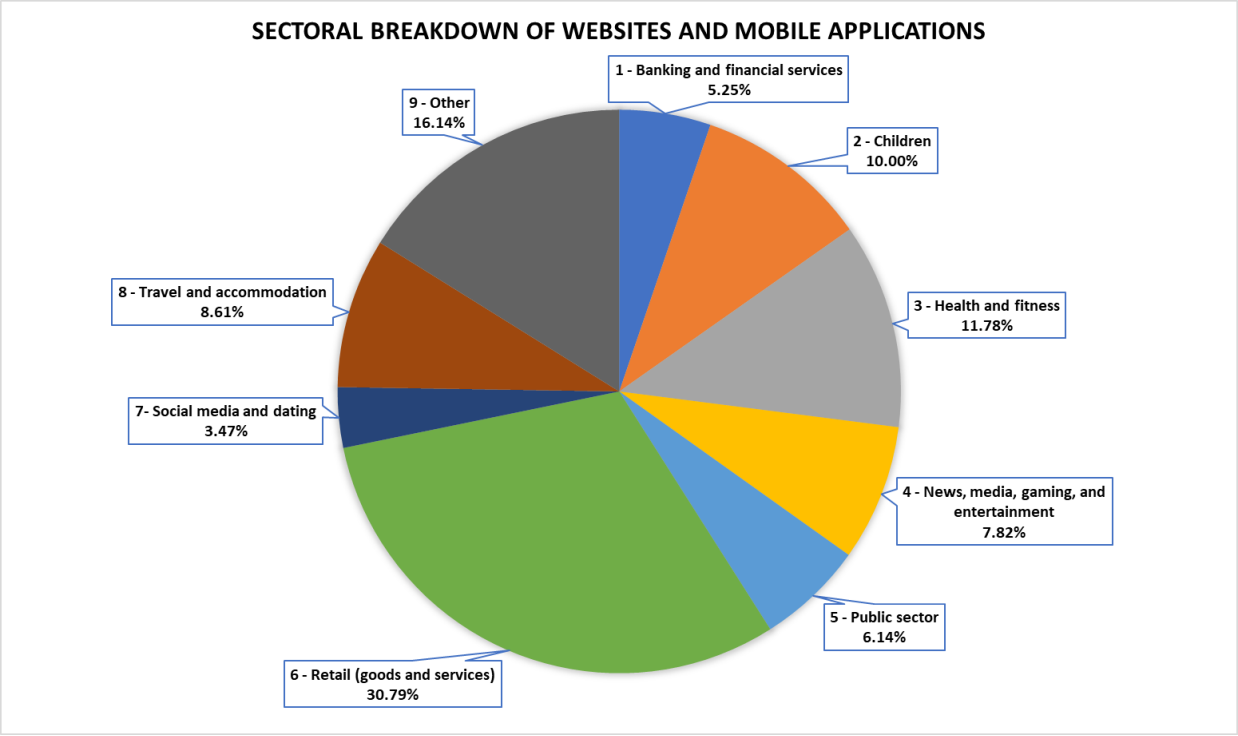


***Figure 1***

## Summary Observations

The Sweep found DDPs on the vast majority website and app examined. For 97% of websites and apps reviewed, across multiple industries, sweepers encountered at least one DDP in their attempt to make privacy-protective decisions or obtain privacy-related information.

The most common DDP observed was complex and confusing language in privacy policies. Sweepers found that 89% of website and app privacy policies reviewed were either excessively long (i.e., over 3,000 words) or contained technical and confusing language, making them difficult to read.

Sweepers also identified frequent use of the DDPs of interface interference and obstruction.

[6] Examples of websites and apps belonging to the "Other" sector, include but are not limited to automotive sites and Internet of Things companion software.

On average, the websites and apps examined used interface interference (e.g., language and visual tools) to influence users to select less privacy-protective options in 43% of interactions.[7] 41% of websites and apps asked sweepers to make privacy choices when they first engaged with the websites and apps. 70% of those (or 31% of all websites and apps swept) made the less privacy-protective options easier to select.

Sweepers also found that websites and apps used obstruction in 39% of interactions to create obstacles between users and their goals, dissuading them from making their intended choices. For example, for websites and apps that contained the option to sign up for an account, sweepers could not find the option to log out of accounts 16% of the time. Furthermore, it took sweepers 3 actions or more to find the option to delete accounts in 27% of the websites and apps swept, and sweepers could not even find the option in another 55%. This shows that deleting accounts is often more difficult than creating them.

In contrast, most websites and apps made their privacy policies easy to find (59% accessible via one click). However, approximately 42% of the policies swept were likely long and required at least a university reading level. 65% of privacy policies also lacked menus for ease of navigation.

The findings suggest that most organizations' platforms are designed to encourage users to make privacy-related decisions that are in the interest of the platform, and potentially not in users' own best interest. This serves to undermine users' autonomy with regard to their privacy.

Below are the aggregated rates of occurrences of the DDPs examined in the Sweep:

| Indicator | Likelihood of Encounter |
|---|---|
| Indicator 1:<br>Complex and Confusing Language | 89% |
| Indicator 2:<br>Interface Interference | 43% |
| Indicator 3:<br>Nagging | 14% |
| Indicator 4:<br>Obstruction | 39% |
| Indicator 5:<br>Forced Action | 21% |

***Figure 2 - Rates of occurrence of DDPs***

[7] For the rest of this report, "interactions" refer to the specified actions sweepers were required to take during their examination of apps and websites (e.g., making decision regarding cookies when prompted by a website is one interaction, locating the privacy policy on an app would be another, etc.).

## Complex and Confusing Language (Indicator 1)

Language plays an important role in allowing users to make informed and meaningful privacy choices. If the language used to explain the organization's practices and privacy settings is highly technical or confusing, users are less likely to understand how their decisions will affect their privacy.[8] Likewise, if the organization's privacy policy is excessively long, users are less likely to read it, and might agree to terms and conditions that they do not understand.[9] Each of these cases could lead users to make decisions that are contrary to their actual privacy preferences.

Complex and confusing language in organizations' privacy policies, present in 89% of cases, is the most common DDP found by sweepers in across all websites and apps they examined that were swept.

Furthermore, participating PEAs reported that 55% of privacy policies on swept websites and apps were more than 3,000 words. In addition, 65% of websites' and apps' privacy policies had no menu or table of contents, making it more difficult for users to find specific information in blocks of text that were often long.

Finally, according to the Flesch Reading Ease Score,[10] 76% of those privacy policies were at an undergraduate reading level or higher, with 20% at, at least, a postgraduate reading level.

[8] Privacy policies may be required to use precise language to meet certain legal requirements, which can contribute to their length and complexity. Nevertheless, organizations should allow their users to quickly review and understand key information impacting their privacy decisions, for example, through a layered approach that enables users to control the level of detail they want to obtain.

[9] European Data Protection Board, "Guidelines 3/2022 on deceptive design patterns in social media platform interfaces: How to recognise and avoid them," at paragraph 26.

[10] The Flesch Reading Ease Score tool assesses the readability of a passage, based on the length of the passage, length of sentences, and the choice of language. A lower score corresponds to a more difficult passage and a higher level of education needed to understand it. The tool does not apply to the languages of choice of all participating PEAs. 21 of the 26 participating PEAs used the Flesch Reading Ease Score to assess the readability of privacy policies.

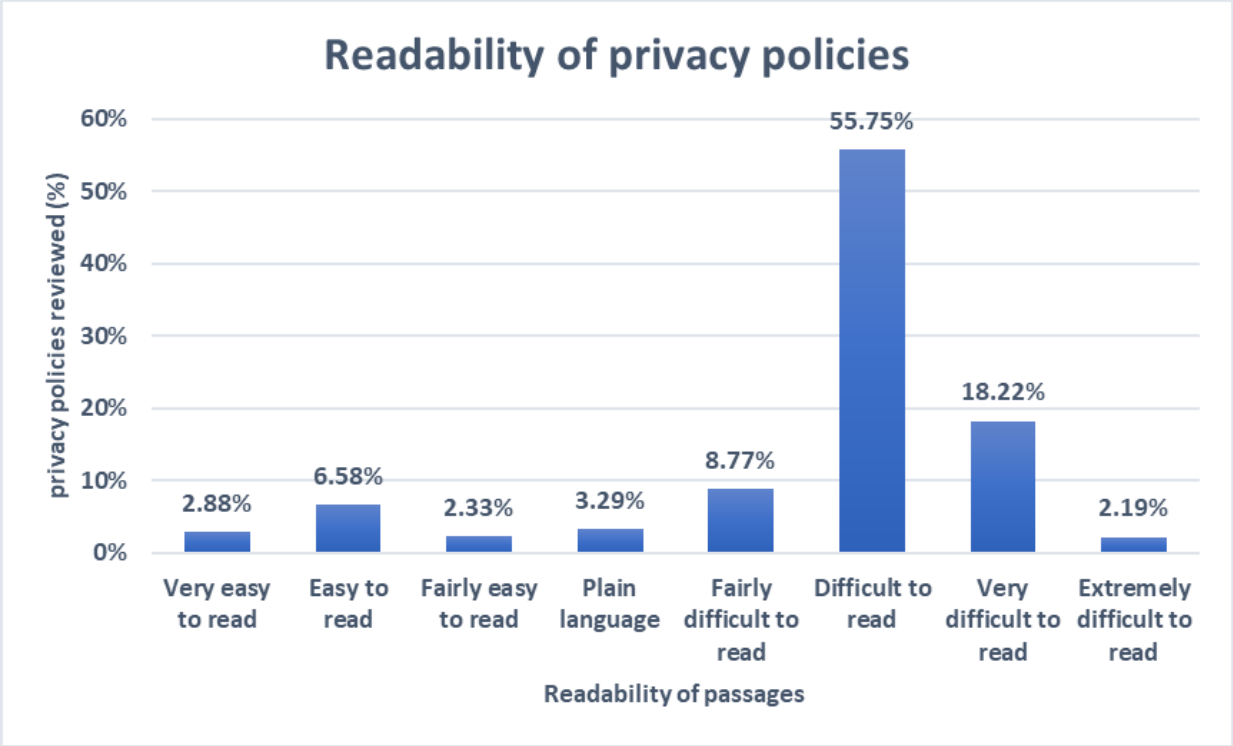


***Figure 3***

## Interface Interference (Indicator 2)

How users react to and interact with privacy options is also largely determined by the way information is presented to them. "Interface interference" refers to the use of design elements and presentation methods that alter users' perception and understanding of their privacy options. Certain subtle platform design elements can interfere with users' ability to make choices that reflect their actual privacy preferences.

Interface interference can influence users' decision-making process through various DDPs, including:

(i) a "false hierarchy": emphasizing certain visual elements and obscuring others, thereby channelling users towards less privacy-protective options (see Figure 4 below);

(ii) "preselection": selecting by default more privacy-intrusive options; and

(iii) "confirm-shaming": using emotive language such that users gravitate towards options favoured by the organization (e.g., "Accept and bring on the deals!" or "What? You don't want to save money?"; also see Figure 5 below).

The Sweep found that, on average, the websites and apps examined used interface interference DDPs in 43% of interactions.

## False hierarchy

When presenting privacy choices to Sweepers, 57% of websites and apps made the less privacy-protective choices easier to select by displaying a false hierarchy. For instance, see Figure 4 below for one representative example, where the website makes the least privacy-protective choice more visible, placing it above the less intrusive option with greater colour contrast.


***Figure 4 - Example of false hierarchy***

Encouraging users to create an account, and in particular to use a third-party social media or email account to sign up for that account, can allow websites and apps to track and/or gather more information about their users. 54% of websites and apps swept made the use of third-party services (such as social media) to sign up for an account more prominent than simply signing up with an email.

## Preselection

Sweepers observed that 48% of websites and apps preselected the less privacy-protective options when they asked users to make privacy choices. Preselection of less privacy-protection options may not reflect users' preferences because a lot of users may not realize they can change the settings or have the time to make those changes.

## Confirm-shaming

Sweepers identified that, of the 34% of apps that prompted them to confirm their privacy settings when engaging with the platform for the first time, 42% (or 14% of all apps swept) used language consistent with confirm-shaming.

Finally, 29% of websites and apps tried to dissuade users from deleting their accounts by using confirm-shaming, in the form of emotionally charged language. Here is a representative illustration:

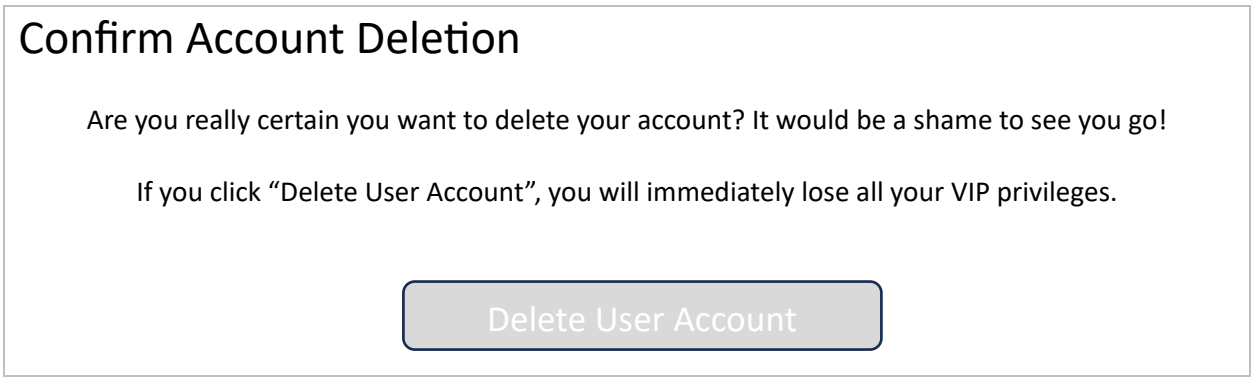


***Figure 5 - Illustration of confirm-shaming***

It is reasonable to ask users to confirm that they want to delete their account. However, using emotionally charged language may influence users to make decisions that are not in their best interests.

## Nagging (Indicator 3)

Nagging is a tactic whereby websites and apps repeatedly prompt users to take a specific action (e.g., revise their privacy settings, or log-in to their account) in favour of the organization’s purposes, which may go against users’ best privacy interests. The repeated requests interrupt the user’s experience and may encourage them to give in to the requests to avoid the nuisance of further prompts.

The Sweep was designed to involve only a brief interaction with the website or app in question, and was therefore not conducive to identifying nagging that might take place over time. However, sweepers found that 35% of websites and apps with an account creation option engaged in nagging by asking users to reconsider their intention to delete their accounts more than once.

## Obstruction (Indicator 4)

Obstruction works by inserting additional steps between users and their goals, dissuading users from, or making them less motivated to, make their intended choices. It can be very effective because it exploits users’ limited time, attention, and/or willingness to navigate websites and apps.

Sweepers examined how websites and apps obstruct users’ experience by creating click fatigue, whereby users are required to make numerous clicks to obtain privacy knowledge or make privacy-protective choices. Sweepers also examined how websites and apps make it difficult for users to cancel or delete their account.

On average, sweepers observed obstruction in 39% of their interactions with websites and apps. The highest rate of occurrence appeared during the account deletion process, where 55% of sweepers were unable to locate the option to delete their account. Even for the 45% of apps and websites where sweepers could find the option to delete their accounts, 27% (or 10% of all websites and apps swept) required users to take inconvenient steps, such as submitting a lengthy form or sending a written request to the organization, to have their account deleted.

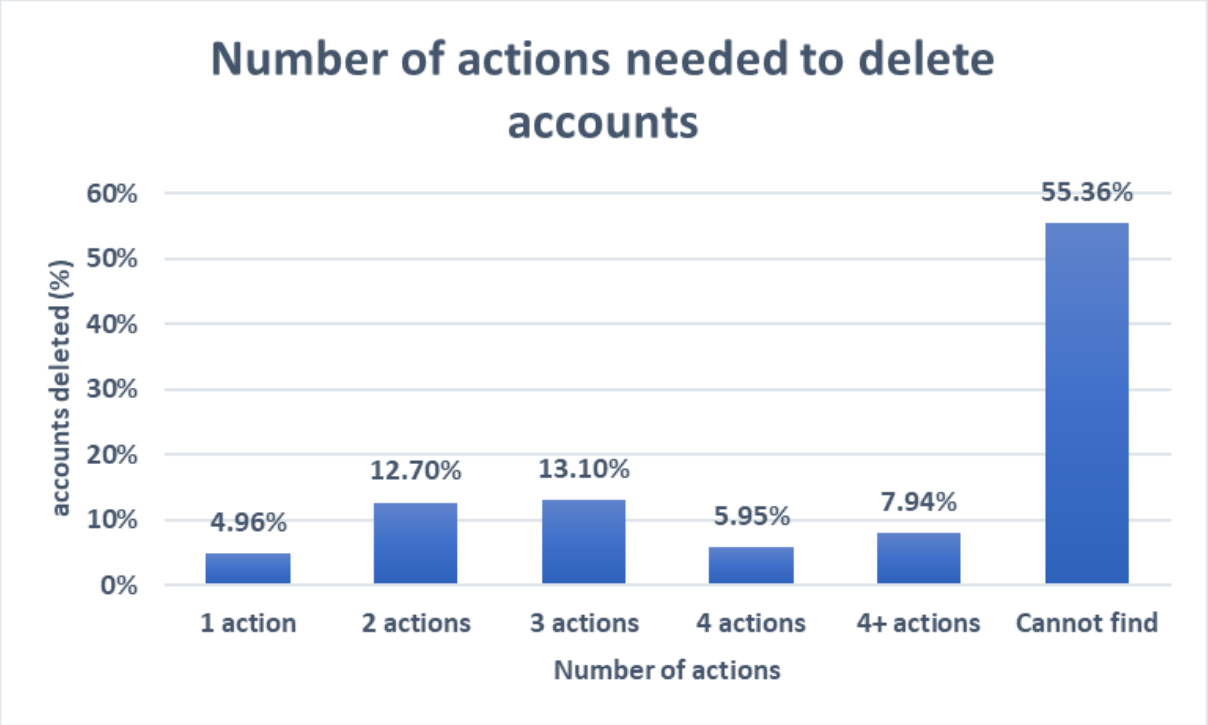


***Figure 6***

Sweepers also encountered obstruction when seeking to change privacy settings. Among the minority of websites and apps that let users adjust their privacy settings (e.g., cookie settings) when they first opened the app or navigated to the homepage of the website, 46% still required additional clicks to refuse the default, more privacy-intrusive settings.

Additionally, there is a significant contrast between websites and apps when it comes to the number of clicks required to locate the privacy policy. While 76% of sweepers were able to find the privacy policy in 2 clicks or fewer on websites, 44% were able to do so while using an app.

77% of sweepers could log out of their website or app account in two clicks or fewer. However, 16% could not find how to log out of their account at all. This is concerning where websites and apps can, in many instances, continue to track users while they remain logged in.

## Forced Actions (Indicator 5)

Individuals may be asked to provide their personal information to receive certain services online. One key privacy and data protection principle is that the collection and use of personal information should be limited to what is necessary.

Forced action DDPs either force users, or trick them into thinking that it is necessary, to provide their personal information to access services where that collection is not, in fact, required to provide the service.

The Sweep examined how websites and apps employed forced action DDPs, such as requiring users to disclose more information than necessary (i.e., "forced disclosure"). Among swept websites and apps that prompted users to make a privacy choice upon opening the platform, 26% deployed this design pattern. To provide an example, the banner below (Figure 7) only offered users the choice to 'accept' cookies in order to browse the organization's website.

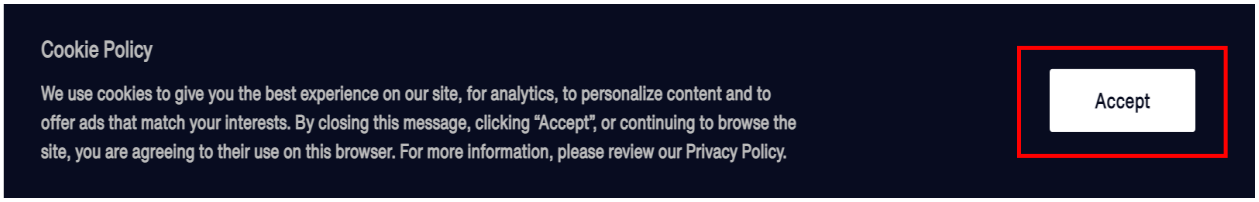


***Figure 7 - Example of forced disclosure***

9% of websites and apps forced users to disclose more personal information to delete an account than they were required to provide when creating the account. In some cases, websites and apps made additional data fields (e.g., home address or full name) mandatory for deleting the account, where this information was not required for account creation.

## Conclusion

The GPEN Sweep aims to encourage organizations to comply with privacy and data protection legislation, while promoting co-operation between privacy enforcement authorities across the globe. Though the Sweep is not in itself an investigation, nor is it intended to conclusively identify compliance issues or legal contraventions, the concerns identified via this exercise may help support targeted education, outreach to organizations and/or enforcement actions in the future.

The outcome of this year's Sweep suggests an extremely high occurrence of deceptive design patterns across websites and apps worldwide, indicating that users are likely to encounter, in the vast majority of cases, at least one DDP when interacting with websites and apps.

Sweepers' observations indicate that many websites and apps have been designed to encourage users to make privacy decisions that may not be in their best interest. The Sweep shows several areas in which organizations could improve the design of their platforms to enable users to better understand and control the use and disclosure of their personal data.

Organizations should design their platforms, including associated privacy communications and choices, to provide users with the ability to make informed privacy decisions. Good privacy design patterns include defaulting to the most privacy-protective settings, emphasizing privacy-protective options, using neutral language and designs to present privacy choices, reducing the volume of clicks required to navigate and adjust users' privacy choices, and providing just-in-time consent options that allow users to make privacy decisions when they are contextually relevant. By implementing privacy-friendly design practices, organizations will offer users of their websites and apps experiences that are free from influence, manipulation, and coercion, and in so doing, can build consumer trust.

## Acknowledgements

On behalf of GPEN, the Sweep Coordinator thanks Dr. Cristiana Teixeira Santos, Assistant Professor in Law and Technology at Utrecht University, for advice in developing the Sweep methodology. [11]

[11] See Dr. Cristiana Teixeira Santos' bio here.

# Appendix A

26 PEAs, from five continents, participated in the Sweep.

The following PEAs provided their results:

1. Access to Public Information Agency, Argentina
2. Office of the Australian Information Commissioner
3. The Commissioner for Data Protection and Freedom of Information, Baden-Wuerttemberg
4. Office of the Privacy Commissioner for Bermuda
5. National Data Protection Authority, Brazil
6. Office of the Information and Privacy Commissioner of Alberta, Canada
7. Office of the Information and Privacy Commissioner for British Columbia, Canada
8. Office of the Privacy Commissioner of Canada
9. Commission d'accés à l'information du Québec, Canada
10. Office of the Privacy Commissioner for Personal Data, Hong Kong, China
11. Office for Personal Data Protection, Macao, China
12. The Commissioner of Data Protection of the Dubai International Financial Centre
13. Commission nationale de l'informatique et des libertés, France
14. Gibraltar Regulatory Authority
15. Office of the Data Protection Authority, Guernsey
16. Garante per la protezione dei dati personali, Italy
17. Personal Information Protection Commission, Japan
18. Jersey Office of the Information Commissioner
19. Office of the Information and Data Protection Commissioner, Malta
20. Instituto De Transparencia, Acceso A La Información Pública Y Protección De Datos Personales Del Estado De México Y Municipios, Mexico

21. National Privacy Commission, Philippines
22. Superintendence of Industry and Commerce, Republic of Colombia
23. Personal Data Protection Commission, Singapore
24. Information Commissioner's Office, the United Kingdom
25. California Privacy Protection Agency, the United States of America
26. Federal Trade Commission, the United States of America