

09/07/2024



GIBRALTAR REGULATORY
AUTHORITY

2nd Floor, Eurotowers 4
1 Europort Road
Gibraltar

Tel: +350 20074636
Fax: +350 20072166
e-mail: info@gra.gi
url: <http://www.gra.gi>

PRESS RELEASE

GPEN Sweep finds majority of websites and mobile apps use deceptive design to influence privacy choices.

The Gibraltar Regulatory Authority ("GRA"), as the Information Commissioner, has taken part in the annual Global Privacy Enforcement Network Sweep (the "GPEN Sweep"). GPEN was established in 2010 upon recommendation by the Organisation for Economic Co-operation and Development (the "OECD"). In an increasingly global market, GPEN aims to foster cross-border co-operation among privacy regulators. Members seek to work together to strengthen personal privacy protections in this global context.

The GPEN Sweep saw 26 privacy enforcement authorities from across the world come together to participate. They collectively reviewed more than 1,000 websites and mobile applications and found that nearly all of them employed one or more deceptive design pattern(s) that made it difficult for users to make privacy-protective decisions.

Deceptive design patterns use features that steer users towards options that may result in the collection of more of their personal data. These patterns may also force users to take multiple steps to find a privacy policy, log out, or delete their account, or present them with repetitive prompts aimed at frustrating them and ultimately pushing them to give up more of their personal data than they would like.

For the first time, the GPEN Sweep was coordinated with the International Consumer Protection and Enforcement Network (the "ICPEN"), which represents consumer protection authorities.

The collaboration recognises the growing intersection between privacy and other regulatory spheres. In the case of deceptive design patterns, it was clear to both privacy and consumer protection sweepers that many websites and apps employ techniques that interfere with individuals' ability to make choices that best protect their privacy or consumer rights.

Both GPEN and ICPEN, who are working together to improve privacy and consumer protection for individuals around the world, published reports today outlining their findings.

Global Findings

Those involved in the GPEN Sweep replicated the user experience by engaging with websites and apps to assess the ease with which they could make privacy choices, obtain privacy information, and log out of or delete an account.

Sweepers evaluated the sites and apps based on five indicators identified by the OECD, as being characteristic of deceptive design patterns.

For each indicator, the GPEN Sweep found:

- **Complex and confusing language:** More than 89% of privacy policies were found to be long or use complex language suited for those with a university education.
- **Interface interference:** When asking users to make privacy choices, 42% of websites and apps swept used emotionally charged language to influence user decisions, while 57% made the least privacy protective option the most obvious and easiest for users to select.
- **Nagging:** 35% of websites and apps repeatedly asked users to reconsider their intention to delete their account.
- **Obstruction:** In nearly 40% of cases, sweepers faced obstacles making privacy choices or accessing privacy information, such as trying to find privacy settings or delete their account.
- **Forced action:** 9% of websites and apps forced users to disclose more personal data when trying to delete their account than they had to provide when they opened it.

The GPEN Sweep was not an investigation, nor was it intended to generate formal findings regarding confirmed violations of privacy legislation. However, as in previous years, concerns identified could not only result in follow-up work such as outreach to organisations but may also lead to the initiation of enforcement action to address identified concerns.

GPEN encourages organisations to design their platforms, including associated privacy communications and choices, in a manner that supports users in making informed privacy choices that reflect their preferences. Good design includes default settings that best protect privacy; an emphasis on privacy options; neutral language and design to present privacy choices in a fair and transparent manner; fewer clicks to find privacy information, log out, or delete an account; and 'just-in-time' contextually relevant consent options.

By offering users online experiences that are free from influence, manipulation, and coercion, organisations can build user trust and make privacy a competitive advantage.

For further information please contact the GRA by telephone on +350 200 74636 or by email on privacy@gra.gi.