GPEN Sweep 2017

'User Controls over Personal information'

October 2017

UK Information Commissioner's Office

ico.
Information Commissioner's Office

Background

The 2017 GPEN Sweep aimed to examine privacy communications and practices in relation to user controls over personal information. Websites and mobile applications have the potential to collect large amounts of personal data from various sources. It is important that users are fully informed about the way in which their data is collected, used, and shared. The theme of 'user controls' allowed participating Privacy Enforcement Agencies (PEAs) to consider whether it was clear from the perspective of the user exactly what information was collected by the website or app, the purpose for which the information was collected, and how this information would be processed, used and shared.

A variety of methodologies were used in the Sweep, including but not limited to:

- Examination of privacy communications available on the website/app - *21 PEAs*
- Creation of accounts/profiles - *12 PEAs*
- Contact privacy officers with a range of specific questions; *3 PEAs*.

To narrow the focus of the sweep, PEAs focused on a particular sector(s) which was of relevance to them, including (but not limited to);

- Education - *7 PEAs*
- Travel - *9 PEAs*
- Retail - *9 PEAs*
- Health - *4 PEAs*
- Social Media - *1 PEAs*
- Gaming/Gambling - *2 PEAs*
- Finance/Banking - *4 PEAs*
- Other - *2 PEAs.*

Note: some PEAs looked at more than one sector.

Summary Observations

Privacy communications across the various sectors were found to be generally very high level and lacked specific detail. However, it was often noted by PEAs that privacy communications were easy to locate on the

website, and the majority of organisations were quite transparent in specifying what information (or categories of information) they would collect.

However, organisations generally failed to specify with whom data would be shared. PEAs also indicated that a number of organisations failed to refer to the security of the data collected and held by them; it was often unclear where data was stored (i.e. which country), or whether any safeguards were in place to protect the user's data. It was also found that just over half the organisations examined made reference to how users could access the personal data held about them. There were some example of good-practice, but these were in the minority.

The overall findings suggest that users of the organisations examined are generally not well informed with regards to what happens to their data once collected. As such, users are unable to exercise their controls easily (such as accessing, retrieving and deleting their data). There is significant room for improvement in terms of specific details contained in privacy communications.

Tombstone Data

Data Protection Authorities who submitted results: 24

Websites/apps examined: 455

***Methodology Note**: Not all Data Protection Authorities ("DPAs") reported on every reporting field. The statistics for this Sweep were developed based on the actual data received for a reporting field as a percentage of those apps/websites swept by those DPAs that reported on that field*.

Collection and use of data (Indicator 1)

Sweepers indicated that around 23% of websites/apps swept failed to specify in their privacy communications exactly what information would be collected from the user, while around 17% failed to gain adequate consent to collect this data.

Based on privacy communications available on the website/app, users were informed that the following information (plus other information)

would be collected either on a mandatory or optional basis by the organisations examined:

- Name: 81% of websites/apps
- Date of birth: 52% of websites/apps
- Address: 51% of websites/apps
- Phone number: 45% of websites/apps
- Email address: 85% of websites/apps
- Usage data: 38% of websites/apps
- Multimedia (audio/video/photo): 8% of websites/apps
- Location: 16% of websites/apps
- Third party information: 9% of websites/apps
- Biometrics: 3% of websites/apps
- Bank/payment details: 25% of websites/apps
- Medical information: 5% of websites/apps
- IP address: 69% of websites/apps

Trends identified in relation to Indicator 1:

- It was noted that the private sector was more likely to address consent in privacy communications than the public sector, which seemed to rely upon their legal authority to collect the information.
- It was noted in many cases that privacy policies often referred to data (or categories of data) that '*may*' be collected.
- Information on how personal data would be used was often generic.
- Some websites/apps made no reference to the collection of information through cookies, despite collecting this information in practice.
- Many websites collect information on an opt-out basis with reliance on implied consent (for example, 'if you use this site you consent to us collecting and processing your information').
- A number of privacy policies used a 'layered' structure, making it clear and easy for the user to understand and follow.
- In addition to a written privacy policy, some websites contained a video, which explained the privacy policy in simple, clear language.

Storage and security of data (Indicator 2)

Based on the findings, only 35% of websites/apps specified in their privacy communications whether they had any safeguards in place to protect the users' data (such as access controls, encryption etc.).

Out of the websites/apps swept, 67% failed to specify where data is stored (i.e. which country).

Trends identified in relation to Indicator 2:

- There was a general trend across the various sectors where privacy communications failed to advise users on how or where their data would be stored.
- It was noted that a couple of websites still referred to Safe Harbor (an agreement which allowed the transfer of European citizens' data to the US), which was revoked by the European Court of Justice in October 2015.

Sharing of data (Indicator 3)

Sweepers found that 51% of websites/apps failed to specify with whom data would be shared, while 25% did not address whether personal information would be disclosed to third parties at all.

Trends identified in relation to Indicator 3:

- It was often unclear with which third parties the data would be shared, and many websites failed to mention that they share data at all.
- Organisations were generally vague as to what information would be shared.
- It was noted that details around the international transfer of data was often unclear. For example, many organisations would note that data may be 'transferred outside the EEA,' but did not specify where or for what purpose.

Deletion of data (Indicator 4)

Around 51% of websites/apps provided instructions on how to remove personal data from their database in their privacy communications.

Only 22% specified whether there was a retention policy in place, with the vast majority failing to provide any explanation as to what would happen with dormant/inactive accounts.

Accessibility of user data (Indicator 5)

Sweepers noted that 56% of websites/apps made it clear to the user how they could access their personal data.

Automated decision-making (Indicator 6)

Around 39% of organisations specified that some decisions would be made by automated means, with 23% noting how the user might contest a decision or request human intervention.

Other findings

- Some organisations referred to outdated legislation.
- A number of the organisations providing services at international level seemed to be unclear as to which legislation or jurisdiction was applicable.
- It was noted that the retailers who issue e-receipts generally failed to provide any information regarding e-receipts on their website.
- In general, it was noted that banking websites did not contain much detail in their general privacy policy. However, policies often noted that further details on how data is used and collected could either be found whilst completing the registration form, or on the relevant terms and conditions provided to customers.

Conclusion

In summary, privacy communications across the various sectors tended to be quite vague, and often contained generic clauses. The majority of organisations failed to inform the user what would happen to their information once it had been provided. It is important that it is clear to users how they can control their information online. It is difficult for a user to exercise their controls when they are not well informed on how to do so. Based on the findings discussed above, users need to be better informed in relation to how they can access or remove the information they provide online, whether the information will be shared and with

whom, and whether the information they provide will be stored in a sufficiently secure manner.