GDPR: its time has come

Karen Renaud
Lynsay Shepherd

The published article is available from doi:
https://doi.org/10.1016/S1353-4858(18)30017-5

GDPR: its time has come

Karen Renaud & Lynsay Shepherd

The new General Data Protection Regulation (GDPR) becomes enforceable from 25 May 2018. The regulation was adopted on the 27th April 2016, so organisations all over Europe have had fair warning.

GDPR requires that the following be provided in a displayed privacy policy: what data is being collected; the justification for such data being collected; how data will be processed; how long data will be retained; who can be contacted to have personal data removed or rendered to the data owner – this includes all information provided by individuals, as well as information observed during their interactions with the company's systems; and the information should be communicated "in concise, easy-to-understand and clear language" [1].

GDPR allows information commissioners to apply heavy sanctions. One of these is *"a fine up to €10 million or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater"*. This ought to be focusing companies' attention on the need to make their privacy policies GDPR compliant.

With about three months to go, how are websites doing in terms of meeting these requirements? We consulted Alexa [2] to identify the top 10 UK websites and we then visited them at the end of January 2018, and viewed their privacy policies. Only two of the top ten: BBC and Wikipedia, satisfy all the requirements. All the others fail in terms of explicitly stating how long they were going to keep the data.

GDPR compliance with some of these mandates is relatively simple. Providing a contact, for example, is straightforward. The 'easy-to-understand language', on the other hand, is not as easy to achieve. Understandability is key. One of the best measures of understandability, which is free and easy to use, is the Gunning Fog Index (http://gunning-fog-index.com/) [3]. This reflects the number of years of education that someone needs to understand a piece of text. We checked the privacy policies of those top 10 websites: one of them required 17 years of education – the equivalent of a Masters degree – which is clearly unrealistic. The BBC's index was 11.34, which requires a high school education. This is far more reasonable. Writers of privacy policies would do well to test their policies, and simplify them accordingly, in order to satisfy this requirement.

The requirement also explicitly states the need for policies to be concise. The longer the displayed policy, the less likely people are to actually read all of it all the way through. One of the websites we examined had a policy comprising 5,260 words and 18.9% were classified by the Gunning Fog Index as complicated (three or more syllables long). One could easily argue that this does not comply with the spirit of the GDPR requirement.

In summary, GDPR is on the horizon and companies have work to do, or risk being fined. Some companies might have to stop trading altogether if the fine is large enough to knock out their reserves. It is not hard to achieve privacy policy compliance when it comes to website privacy policies, but it will take a bit of effort and some serious editing to make it as easy as possible for people to understand the policy itself.

The time has come – get ready!

[1] Information Commissioner's Office, "Preparing for the General Data Protection Regulation (GDPR) - 12 Steps to Take Now," 2018, https: //ico.org.uk/media/1624219/preparing- for- the- gdpr-12- steps.pdf.
[2] https://www.alexa.com/topsites/countries/GB
[3] http://gunning-fog-index.com/