Nomos
société d'avocats

nomosnetcom.fr **December 2017**

GPEN Sweep day 2017: privacy policies of websites and apps are generally too vague and inadequate

[PERSONAL DATA]
GPEN Sweep 2017 report by the UK Information Commissioner's Office, published in October 2017

The Global Privacy Enforcement Network (GPEN) is an international network of data protection authorities, created following a 2007 recommendation of the OECD. To date, the GPEN comprises 49 members throughout the world.

Each year, the GPEN organizes an international "sweep day" where participating authorities investigate specific practices or particular areas of the data protection legislation. The 2017 Sweep day aimed to examine privacy communications and practices in relation to users' control over personal information. For this purpose, 24 member authorities examined 455 websites and applications, including in retail, finance, banking, travel, social media, education etc.

The GPEN's general findings are that websites and apps' privacy notices are too vague and generally inadequate. Therefore, the GPEN considers that users are unable to exercise their control easily (such as accessing, retrieving and deleting their data).

The GPEN focused on six main "indicators":

- **Collection and use of data**: generally, privacy policies are not specific enough about what data is collected, and for which purposes.

  The GPEN noted in particular that many privacy policies merely refer to data that "may" be collected, which is inconsistent with the obligation to deliver specific and clear information. It also stressed that some websites or apps make no reference to the use of cookies.

  On the plus side, the GPEN praised the use of layered structures in privacy policies, and the recourse to additional means of information such as explanatory videos.

- **Storage and security of data**: the main trend observed by the GPEN is that websites and apps generally fail to inform users on how and where their data is stored.

- **Sharing of data**: as in the overall analysis, information as to with which third parties personal data is shared – including in particular non EEA third parties – was found insufficiently specific for the majority of the websites and apps investigated.

Deletion of data: more than two-third of the websites and apps controlled do not inform user on their retention policies. This can however be explained, because – as far as EU websites and apps are concerned – the obligation to specify retention periods of the data collected was not part of directive 95/46. GDPR does comprise such an obligation, which will be enforceable as of 25 May 2018. In addition, France has modified its data protection act in October 2016 to include this obligation as well.

- **Accessibility of user data**: here, the GPEN noted that more than half of the websites and apps made it clear to the user how they could exercise their right of access.

- **Automated decision-making**: the GPEN observed that only 23% of the websites and apps which specify that some decisions would be made by automated means, inform users on how they might contest the decision or request human intervention.

In Europe, websites and apps will have to update their privacy policies in order to comply with the GDPR which enters into application in less than 6 months, on 25 May 2018. The French data protection authority (CNIL) stated that this year's sweep will help data protection authorities prepare for future joint operations taking place once GRPD is applicable.

Sylvain NAILLAT