Alexey Muntyan,
Lawyer and expert with ten years of experience in Data Protection field

The General Data Protection Regulation (GDPR) (EU) 2016/679[1] is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas.

The territorial scope of the GDPR applies to the processing of personal data of data subjects who are in EU/EEA where the processing activities are related to the monitoring of their behaviour as far as their behaviour takes place within EU/EEA (GDPR, Art. 3(2)).

In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes (GDPR, Rec. 24).

Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them (GDPR, Rec. 30). According to the European Commission[2], examples of personal data are “location data (for example the location data function on a mobile phone), an Internet Protocol (IP) address, a cookie ID, the advertising identifier of your phone”.

Article 4(11) of the GDPR stipulates that consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The Article 29 Working Party guidelines on consent provide guidance[3] on how this should be interpreted.

Thus, taking into account the findings of this article, it seems possible to draw the following conclusions:

1. Some activities of browser extensions providers may be considered in the context of the GDPR requirements, if these extensions are installed and used on the browsers of data subjects in EU/EEA.

2. The qualification of user data – location data, IP address, cookie ID – as "non-personal" or "anonymized" can be seriously criticized from the GDPR perspective, which automatically casts doubt on compliance with applicable GDPR requirements regarding the subject's consent to the processing of his or her personal data.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[2] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
[3] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051