

(English version)

**Question for written answer E-002546/24
to the Commission
Afroditi Latinopoulou (Pfe)
(14 November 2024)**

Subject: Reviewing the classification of IP addresses as personal data

Under Article 4 of the GDPR, IP addresses are considered ‘identification numbers’, thus constituting personal data. However, an IP address is simply a unique number that is assigned to devices connected to the Internet. There is no direct link with natural persons. Linking an IP address with the identity of a specific person requires either the user’s declared consent or a legal process to be conducted through the relevant Internet service provider.

What is more, most users have a dynamic IP address that changes regularly. This is why many technologically advanced countries such as Australia, Japan and certain states in the US do not consider IP addresses to be personal data.

The fact that they are considered such in the EU has a negative impact on businesses because users have to consent to their IP address being processed, even though this address alone cannot reveal a person’s identity. While we acknowledge that the user’s express consent is needed for actual personal data that reveals a user’s physical identity, IP addresses cannot be considered as such.

In view of this:

1. What solution does the Commission propose to settle the fundamental technical problem of IP addresses being considered personal data when they do not automatically reveal any personal physical attribute that would make the user identifiable?
2. Can the Commission make the necessary amendment to the GDPR, removing the classification of IP addresses as personal data?

Submitted: 14.11.2024

**Answer given by Mr McGrath on behalf of the European Commission
(19 February 2025)**

The definition of personal data in Regulation (EU) 2016/679 ⁽¹⁾ (GDPR) is technologically neutral and broad to prevent creating a serious risk of circumvention of the protection of personal data ⁽²⁾. Article 4(1) GDPR defines personal data as ‘*any information relating to an identified or identifiable natural person*’, including an online identifier that identifies the person directly or indirectly.

Online identifiers, such as cookies and Internet Protocol (IP) addresses, combined with other information may be used to create online profiles of natural persons and identify them ⁽³⁾.

Whether an IP address is personal data within the meaning of Article 4(1) GDPR depends on whether it can be linked to an identified or identifiable natural person.

That is not necessarily always the case and depends on the specific circumstances of the case. In that respect, account must be taken of all the means reasonably likely to be used to identify the person, looking at all objective factors, such as the cost, the amount of time required for identification, taking into consideration available technology ⁽⁴⁾.

The Court of Justice of the EU found on several occasions that IP addresses constituted personal data because the user of the IP address could be identified by the controller at issue ⁽⁵⁾.

In the second report of the application of the GDPR ⁽⁶⁾, the Commission did not conclude that the definition of personal data should be amended.

⁽¹⁾ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1-88.

⁽²⁾ See for more Recital 15 GDPR.

⁽³⁾ See for more Recital 30 GDPR.

⁽⁴⁾ See for more Recital 26 GDPR.

⁽⁵⁾ See for example C-470/21 and C-604/22.

⁽⁶⁾ Communication from the Commission to the European Parliament and the Council Second Report on the application of the General Data Protection Regulation, COM/2024/357 final.

Regardless of their nature as personal data, where IP addresses are stored or accessed from the user's terminal equipment, Article 5(3) of Directive 2002/58/EC ⁽⁷⁾ applies.

That provision protects the confidentiality of users' terminal equipment. It requires consent for the storage of or access to information (both personal and non-personal) stored in the terminal equipment, unless it is carried out for the sole purpose of carrying out the transmission of a communication or if it is strictly necessary for the provision of an information society service explicitly requested by the user ⁽⁸⁾.

⁽⁷⁾ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37-47, see in particular Recital 28.

⁽⁸⁾ See also EDPB, Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive.