European Parliament
2024-2029

Committee on Petitions

16.1.2025

NOTICE TO MEMBERS

Subject: Petition No 0982/2024 by N.U. (Finnish) on deletion of all personal data from the registry of health authorities

1. Summary of petition

The petitioner states that it is not in the public interest that personal data be kept in several different registers in Finland without the knowledge of the individuals concerned. He cites the examples of health authorities in Finland, such as the Finnish Institute for Health and Welfare and the Finnish Social and Health Data Permit Authority. He claims that this is not only a security risk, but could also be target of cyber-attacks by non-EU countries. Therefore, he asks that the use of personal data by these authorities be fully based on consent and that all personal data that are not needed be deleted.

2. Admissibility

Declared admissible on 22 November 2024. Information requested from Commission under Rule 233(5).

3. **Commission reply**, received on 16 January 2025

The petition

The petitioner asks that it must be possible to delete all personal data held by Finish authorities if they do not need them in the performance of their activities. This concerns, for instance, health authorities doing research, such as the Finnish Institute for Health and Welfare (THL), and the Finnish Social and Health Data Permit Authority (Findata). According to the petitioner, the processing of personal data by those authorities should be entirely based on consent. The petitioner also takes the view that it is not in the public interest that personal data is stored in several registries without data subjects' knowledge and consent.

The petitioner alleges that this is not only a data security risk but also provides a target for a cyberattack by a non-EU country.

The Commission's observations

The General Data Protection Regulation (GDPR)[1] sets the rules on the protection of personal data as well as the rights of individuals as concerns their personal data. The Regulation provides for all the necessary safeguards to protect personal data of individuals in the EU. It establishes a set of comprehensive rules for the protection of personal data, which apply directly to public and private organisations in the EU.

Pursuant to Article 5(1)(a) GDPR, personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. The processing of personal data is lawful only where at least one of the six legal bases set out in Article 6(1) GDPR is fulfilled. The consent of the data subject is one of the possible legal bases, but not the only one. Typically, public bodies rely often on another two legal bases, namely: "processing is necessary for compliance with a legal obligation to which the controller is subject" (Article 6(1)(c) GDPR) or "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" (Article 6(1)(e) GDPR). Article 6(3) GDPR provides that where processing is based on Article 6(1)(c) or (e), the basis for the processing shall be laid down by Union or Member State law. In addition to the requirement to rely on a valid legal basis, the processing of special categories of personal data (such as data concerning health) is authorised only if one of the conditions listed in Article 9(2) GDPR is met.

Consequently, if Finnish law were considered as providing an appropriate legal basis for the processing of personal data by the authorities concerned and as fulfilling one of the conditions under Article 9(2) GDPR, including the provision of adequate safeguards, the consent of the data subjects would not be needed.

It must be noted that the two Finish authorities explicitly mentioned by the petitioner (i.e. THL and Findata) have provided information on their websites about the legal bases on which their various processing operations rely. They include points (a), (c) and (e) of Article 6(1) GDPR, depending on the purposes of the processing.[2]

As regards the petitioner's request that the personal data held by the authorities concerned must be deleted if they do not need them in the performance of their activities, this is reflected in the 'storage limitation' principle enshrined in Article 5(1)(e) GDPR. According to this principle, the storage of the data must be limited to what is strictly necessary for the purposes pursued, and in practice it should be as short as possible. It follows that the authorities concerned, acting in their capacity as controllers in the sense of Article 4(7) GDPR, have the duty to delete the personal data once the purpose of the processing has been fulfilled, unless EU or Member State law requires further storage or the data are stored for longer periods,

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), *OJ L 119, 4.5.2016, p. 1–88*.
2 https://thl.fi/en/about-us/data-protection
https://findata.fi/en/about-findata/data-protection-and-the-processing-of-personal-data/#General-information-and-frequently-asked-questions-about-secondary-use

insofar as they will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR.

Concerning the petitioner's allegation that the storage of the data on several registries would cause a security risk, it must be borne in mind that the GDPR requires both controllers and processors to have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the personal data being processed (Articles 5(1)(f) and 32 GDPR). Consequently, the ability to prevent, detect, address, and report a data breach (including more complex and severe breaches like cyberattacks) in a timely manner should be seen as essential elements of these measures.

Furthermore, the GDPR explicitly introduces the accountability principle according to which the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to processing of personal data (Article 5(2) GDPR).

Finally, the monitoring and enforcement of the application of the GDPR falls within the competence of the national data protection authorities and courts, without prejudice to the competences of the European Commission as guardian of the Treaties.

Conclusion

The Commission considers that the petitioner's request for consent as a legal basis for the processing of personal data by the Finish authorities concerned is not justified if that processing relies on another valid legal basis, such as national law which provides the necessary conditions and safeguards. Besides the requirement to respect the principle of lawfulness, the GDPR imposes a range of other obligations to the authorities concerned, acting in their capacity as controllers. Notably, in line with the 'storage limitation' principle, the authorities concerned have the duty to delete the personal data that are not needed anymore for the purpose of the processing, subject to the applicable data retention requirements. The authorities concerned are also under the obligation to ensure a level of data security that is appropriate to the risk, which means that they must take all the measures necessary to prevent a cyberattack. Compliance with those obligations would guarantee a high level of personal data protection.