European Data Protection Board

Anu Talus
Chair of the European Data Protection Board

Silvia Lorenzo Perez
Centre for Democracy and Technology Europe (CDT Europe)
sperez@cdt.org

Brussels, 11 February 2026

by e-mail only

Dear Ms. Silvia Lorenzo Perez,

Thank you for your letter of 26 June 2025 regarding your concerns on spyware abuse cases in the European Union ('EU'). Please be assured that the European Data Protection Board ('EDPB') is also vigilant as to the effects of the use of such spyware on civil society and fundamental rights and follows reports on the abuse of such products closely, in particular where this use is directed against NGOs or journalists. The protection of journalists and their sources is of utmost importance for the freedom of the press and thus for the protection of fundamental rights, the rule of law and democracy as such. The European Media Freedom Act[1] includes a general prohibition of such intrusive surveillance software in devices, materials and digital tools used by media service providers, including journalists, with narrowly defined exceptions for the investigation of certain offences listed in the European Arrest Warrant[2] or other serious crimes, and subject to strict substantive and procedural conditions.

The EDPB is the independent European body, which contributes to the consistent application of data protection rules throughout the EU by issuing guidance on data protection law and promoting cooperation between the EU data protection authorities ('DPAs'). Under the General Data Protection Regulation ('GDPR'), the investigation and enforcement of data protection rules in individual cases, including regarding the alleged use of spyware by private entities, falls under the competence of the DPAs.

In matters relating to any processing operations carried out by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, the competence of the DPAs would be based on the Law Enforcement Directive ('LED').[3] Furthermore,

[1] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act) (hereinafter referred to as 'European Media Freedom Act') (OJ L, 2024/1083, 17.4.2024).
[2] See Article 2(2) Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) (OJ L 190 18.7.2002, p. 1).
[3] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,

the ePrivacy Directive[4] also provides rules for the protection of the users' right to privacy and confidentiality of their electronic communications, as well as the integrity of their terminal equipment.[5] In this regard, the EDPB has issued guidelines on the applicability of Article 5(3) of the ePrivacy Directive.[6] The EDPB notes that while some data processing operations, mainly related to the deployment of such software, might fall within the scope of Union law, any processing activities relating to national security fall outside of the scope of Union law.[7] Yet, it is important to stress that Member States cannot abusively invoke national security to escape from the application of EU law[8].

It should also be noted that whenever spyware is used to process personal data in the context of activities falling within the scope of the EU data protection law, both national authorities and private entities are obliged to comply with the obligations set out therein. This includes inter alia identifying a valid legal basis for the processing of personal data, complying with the data protection principles and respecting the data subjects' rights. The CJEU case law states that access, retention and further use of personal data by public authorities for surveillance purposes must not exceed the limits of what is strictly necessary.[9]

While the EDPB's competences are limited where the use of such spyware is related to national security aspects, the EDPB is mainly competent insofar spyware is deployed for processing purposes falling under the scope of the GDPR and the LED. At the same time, the EDPB does not have the same competences, tasks and powers as national data protection authorities. Indeed, at national level, the assessment of alleged infringements of the EU data protection framework, including regarding the use of spyware by private entities, falls first and foremost within the competence of the responsible and independent national supervisory authorities.

In addition, the principle of transparency may be of particular relevance in this regard, as it requires data subjects to be made aware of the risks, safeguards and rights in relation to the processing of their personal data in a concise, intelligible and easily accessible form, using clear and plain language. While in certain limited circumstances, Member States may restrict the information obligations under Articles 12 to 14 GDPR pursuant to Article 23 GDPR, such restrictions must be laid down in law, be

---

and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, pp. 89–131).

[4] 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 (OJ L 201, 31.7.2002, pp. 37–47).

[5] In particular, Article 5(1) and 5(3) of the ePrivacy Directive provide that, as a rule, the users' prior consent is required for the storing of information, or the gaining of access to information already stored, in their terminal equipment.

[6] EDPB Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, adopted on 7 October 2024.

[7] Please note that regarding the ePrivacy Directive, the CJEU has ruled that its Articles 1(3), 3 and 15(1), read in the light of Article 4(2)TEU, must be interpreted as meaning that national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security falls within the scope of that Directive (CJEU, Judgment of 6 October 2020, C-623/17, Privacy International, paragraph 49). It should also be noted that, in any event, as regards national security considerations, Member States are still bound by the guarantees of the European Convention of Human Rights.

[8] Judgment of the CJEU of 4 June 2013, ZZ v Secretary of State for the Home Department, C-300/11, ECLI:EU:C:2013:363, paragraph 38.

[9] CJEU Case C-623/17, Privacy International, paragraph 81.

necessary and proportionate in a democratic society, and respect the essence of the fundamental rights concerned.[10]

The EDPB will continue to pay attention to the use of such spyware for surveillance purposes including when necessary, by analysing the use of these and other similar technologies. The EDPB will also continue to support cooperation among DPAs in order to ensure the fundamental rights of EU citizens, in particular their right to privacy and data protection.

Yours sincerely

Anu Talus

[10] More information on this principle can be found in Article 29 Working Party's Guidelines on transparency under Regulation 2016/679, as endorsed by the EDPB, available at: https://www.edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en

European Data Protection Board
Rue Wiertz, 60
1047 Brussels