WHSIMION
& PARTNERS

DATA PRIVACY UPDATES

June 2025

whsimionpartners.ro

SANCTIONING PRACTICES

ANSPDCP (Romanian DPA)

Surveillance system without prior consultation of employees – controller fined EUR 3,000

FACTS

The DPA found, following some notifications, that there was no mandatory, complete and explicit prior information of the company's employees after it implemented audio-video surveillance systems. Moreover, the controller could not prove that it had responded to requests to exercise the rights provided by the GDPR. It also turned out that the controller was not aware of the installation of a filter for forwarding messages from one email address to another, which led to the disclosure of some documents.

WHAT SHOULD YOU DO?

- Inform employees completely and early about audio-video surveillance. Any form of monitoring, including video cameras or audio recordings, must be accompanied by prior, clear and accessible information, according to Articles 13 and 14 of the GDPR.
- Regularly check your internal email security policies. The implementation of features such as automatic email forwarding without the controller's knowledge indicates lack of control over the IT infrastructure. It is essential to have clear and auditable procedures in place for managing access and resolving requests for access, rectification or deletion.

GPDP (Italian DPA)

Messenger and WhatsApp chats used for dismissal – controller fined EUR 420,000

FACTS

The Italian DPA fined the company for illegally processing the personal data of an employee, which was later used as a justification for her dismissal. The company used content from the employee's Facebook profile, as well as from private conversations on Messenger and WhatsApp, obtained through screenshots sent by colleagues or a third party.

WHAT SHOULD YOU DO?

- Respect the boundary between the professional and private spheres in disciplinary investigations. Even if the data comes from seemingly accessible social networks or applications, it cannot be used for disciplinary purposes without a clear legal basis and without respecting the principles of confidentiality.
- Assess the proportionality and relevance of the processing in relation to the purpose pursued. Personal data may only be processed to the extent that it is strictly necessary and relevant for a clearly defined legitimate purpose. Excessive or arbitrary use of personal information – even from seemingly public sources – violates GDPR principles.

Datatilsynet (Norwegian DPA)

Audit of 6 websites on pixel tracking – one controller fined approximately EUR 21,100

FACTS

All six sites illegally transferred visitors' personal data to third parties without a legal basis. Even sensitive information (regarding health, religious orientation and about children) was disclosed without consent or proper information. Visitors were informed that they were anonymous, even when they were not. Misleading messages, complex wording in cookie banners, and pressure to opt-in have been identified as problematic practices.

WHAT SHOULD YOU DO?

- Conduct a regular audit of tracking technologies. Check whether the pixel tracking technology collects personal data and remove it or implement a legal basis and appropriate information methods.
- Ensure real transparency in cookie banners. Clearly inform users about what is being collected, who has access, and obtain explicit consent, especially for sensitive and minors' data.

LEGISLATIVE UPDATES AND GUIDELINES

CNIL (French DPA) publishes guidelines on development of AI systems, in relation to legitimate interest

In order to ensure a stable regulatory framework, focused on the principles promoted by the GDPR, the French authority has published several steps for operators to consider in the development phase of AI systems in order to be able to justify their processing of personal data on the legal basis of legitimate interest.

- Step 1 – defining an objective of the AI system. A clear objective allows data minimisation to be respected.
- Step 2 – determining responsibilities. This stage refers to the designation of roles according to the GDPR, i.e. the designation of the controller and, possibly, the processor. The "roles" provided for by the AI Regulation must also be taken into account.
- Step 3 – definition of the legal basis for processing. Here, legitimate interest has several particularities that must be taken into account for legitimate processing.
- Step 4 – verification of the possibility of re-use of personal data. This occurs when the controller wants to process a personal database that it already has. It must be verified whether the initial processing and its particularities allow this reuse.
- Step 5 – minimising the data used. In other words, the objective defined in step 1 must be achieved by processing as little personal data as possible. Therefore, it could be useful to go through a trial period or to request an informed opinion from an ethics committee.
- Step 6 – establishing a data storage duration. This duration must be determined in relation to the defined objective. Longer storage may be justified by reasons such as conducting audits or solving problems related to system biases.
- Step 7 – conducting a personal data protection impact assessment (DPIA). It is an important step, especially when sensitive data is collected, when the volume of data is very large or when several databases are cross-referenced.

EDPB publishes the final version of Guidelines 02/2024 on Article 48 GDPR

- Any judicial or administrative decision in a third country that requires the transfer or disclosure of personal data by an EU entity is ineffective in the absence of a valid international agreement (e.g. treaty on legal assistance through good cooperation) and compliance with the provisions of Chapter V of the GDPR (Art. 44–49).
- It applies to requests coming directly from courts, tax, security or regulatory authorities in third countries to controllers or processors in the EU.
- Article 48 does not apply automatically in the absence of an international legal instrument. Requests outside of such instruments cannot be recognised and, if answered, this constitutes an illegal transfer of data.
- Some practical tips:
  - Check for an applicable international agreement (e.g. Mutual Legal Assistance Treaties).
  - In the absence of an agreement, you can apply to the requesting authority to address through the appropriate legal channel to the national competent authority.
  - Ensure that the transfer complies with lawful processing principles and requirements for the international transfer of personal data.

WHSIMION
& PARTNERS

FACTS

For more information:

Cosmina Maria Simion
Managing Partner
cosmina.simion@whsimionpartners.ro

Petruș Partene
Managing Associate
petrus.partene@whsimionpartners.ro

whsimionpartners.ro