

# CJEU Warns that Protection for Special Categories of Personal Data also Applies to Inferred Information

19 August 2022

On 1 August 2022, the Grand Chamber of the European Court of Justice (CJEU) issued a preliminary ruling in case C-184/20 on the questions referred to it by the Regional Administrative Court of Vilnius, Lithuania (the **Referring Court**), concerning the interpretation of special categories of personal data within the meaning of Article 9 of the General Data Protection Regulation 679/2016 (the **GDPR**).

The question before the CJEU concerned a requirement under Lithuanian law for a director of an establishment receiving public funds to declare his private interests. The Chief Ethics Commission (**CEC**) found that the director, by failing to lodge such declaration, infringed the relevant Lithuanian law. The director brought an action for annulment of the CEC's decision before the Referring Court, arguing that the obligation to disclose the private information violated the GDPR. The Referring Court sent some questions to the CJEU for a preliminary ruling.

The first question sought to know whether the mandatory publication of private information was compatible with Articles 6(1)(c) and (e) and 6(3) of the GDPR. In this respect, the CJEU held that the relevant Lithuanian law complies with the conditions set out in Articles 6(1)(c) and 6(3) GDPR, notably that it meets an objective of public interest and is proportionate to the legitimate aim pursued (*i.e.*, guaranteeing impartiality of persons working in the public service).

However, the CJEU also considered that it had to assess whether it is *necessary* to publish on the CEC's website all the personal data contained in the declaration in order to achieve the objectives of general interest defined in the relevant Lithuanian law. After balancing the objective of general interest against the fundamental rights at issue, the CJEU found that the publication online of the majority of the personal data in such declaration does not meet the requirements of a proper balance.

With its second question, the Referring Court sought to know whether Article 9(1) GDPR applied to personal data that could "*disclose indirectly*" sensitive information about a person. In particular, the relevant Lithuanian law required the publication of the name of the partner of the public official, which could indirectly reveal the person's sexual orientation. Pursuant to Article 9 of the GDPR, the processing of special categories of personal data (*e.g.*, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or data concerning health) is prohibited, unless one of the exceptions (as listed in the second paragraph of Article 9 GDPR) applies.

According to the CJEU, the concept of special categories of personal data must be interpreted broadly as it is the objective of the GDPR to ensure a high level of protection of the fundamental rights and freedoms of natural persons.

As a result, the CJEU ruled that, although the personal data at issue are not, inherently, special categories of personal data under the GDPR, it is possible to deduce from the name-specific data relating to the partner of the declarant certain information concerning the sex life or sexual orientation of the declarant. Therefore, the publication of these data indirectly reveals sensitive information and must therefore be interpreted as constituting a processing of special categories of personal data, which falls under the prohibition of Article 9(1) GDPR.

This decision may have various consequences. First, the most obvious take-away is that individuals whose information is published online could oppose such publications if sensitive data can be inferred and the publication is not strictly necessary for the purpose pursued.

However, the judgment also has more far-reaching consequences for various organisations, which will need to review whether their databases may infer special categories of data. This may be particularly relevant

for advertisers and other organizations that keep profiles of data subjects, or track their location. Such inferences may be particularly hard to eliminate when using machine learning or AI. Removing sensitive categories of data from a database may not suffice to escape the requirements of Article 9 of the GDPR. Instead, controllers will also need to assess whether the application does not use any proxies or inferences of sensitive data. If the processing operation is liable to fall under Article 9 of the GDPR, it must be justified by one of the legal bases permitting the use of special categories of data, such as consent, which can have a significant impact on these activities.

The full CJEU judgment can be found [here](#).