



ELB Blogpost 38/2022, 21 September 2022

Tags: Data protection, GDPR, proportionality test, sensitive data, transparency

Topics: Data protection and digital governance

Comment to Case C-184/20 and the perils of a broad interpretation of Art. 9 GDPR

By Giacomo Delinavelli

On 1 August 2022, in [Case C-184/20](#), by responding to a referral procedure brought by the Regional Administrative Court of Vilnius, Lithuania, the Court of Justice (hereinafter Court) addressed two prominent issues of data protection law, namely the balancing of transparency obligations with data protection rights, as well as the extent of protection of – potentially – sensitive data.

This judgement has attracted plenty of interest from the data protection community, and generated speculations regarding the consequences of this case. In this blog post, it will be argued that although transparency obligations, conceived to fight against corruption, can conflict with the rights of privacy and data protection, the key for solving this conflict lies in a sophisticated and complex proportionality test, that keeps into account all the specific legal and factual elements of the case.

Moreover, in the second part of this blog, it will be shown, contrarily to what stated in several [hot](#) takes to this judgement, how this ruling, in the part concerning the interpretation of personal data that can be intended to reveal sensitive data, does not provide sufficient clarity for determining what data can be considered potentially sensitive.

The background of the case, in brief

OT is the administrator of a company that has received EU funding. Pursuant to Lithuanian law, individuals who receive EU funding, even if they do not have public roles, are subject to provide a declaration of private interests (DPI). This declaration is aimed at fighting corruption and ensuring good government. Among other things, the DPI indicates

information about the declarant's spouse or cohabitant, as well as any transactions above €3.000 of value occurred in the previous 12 months (para 29). The DPI is published on the website of the chief ethics commission of Lithuania (para 30).

In consideration of the legal obligations just mentioned, the Vilnius administrative court reveals a possible conflict between the envisaged transparency obligations and the right to privacy and data protection, enshrined in art. 7 and 8 CFR. Therefore, the following questions are referred to the CJEU:

Questions referred, summarised

(1) With the first question, it was asked to what extent the publication, online, of OT's declaration of private interests could rely on article 6(1) and (3) [GDPR](#), as valid legal basis for the data processing. And (2) with the second question, it was asked whether the publication of the name of OT's partner could be processed in accordance with the limits and conditions set out in article 9(1) and 9(2)(g) GDPR.

Regarding the first question, the CJEU points out that the fundamental rights envisaged in the CFR in general, and the fundamental rights of privacy (art. 7) and data protection (art. 8) are not absolute rights, and in case of competing interests, they should be balanced against other legitimate rights and interests, pursuant to recital 4 GDPR.

For, the very first step that the Court undertakes is to inquire the legitimacy of the interest opposing the rights of privacy and data protection (para 74–80). In this case, the Court highlights how transparency, impartiality and fight against corruption is a legitimate interest, recognised as a general objective that Member States have undertaken both at [EU](#) and [international level](#).

Once the legitimacy and importance of the opposing interest have been recognised, the CJEU assumes that the DPI could be processed on the basis of Art. 6(1)(c) GDPR – fulfilment of a legal obligation. However, as envisaged in Art. 6(3) GDPR, when processing data on the basis of 6(1)(c), certain conditions apply. The processing should be based on a national or European legal provision and be proportionate to the interests pursued.

The test of proportionality (*lato sensu*) is composed of three steps of analysis: suitability, necessity and [proportionality *stricto sensu*](#).

Regarding the **suitability** of the measures, the Court considers placing information online in order to achieve the competing interests of transparency and fight against corruption to be appropriate (para 82-84), thus passing the suitability test.

Next, regarding the **necessity** of the measures, the Court considers whether less restrictive measures to the rights of privacy and data protection would have been capable of achieving the envisaged result (para 85-97). For the Court, this assessment is contextual.

It will be based on certain elements that characterise the facts at hand, such as the presence of other measures designed to prevent conflicts of interests, the hierarchical positions of the declarant, the relevance of the data requested, their nature and the presence of safeguards (para 86). One particularly concerning aspect is to justify the necessity to publish the DPI online, which, potentially, could be seen by an unlimited number of people for an unrestrained amount of time.

The Court recognises that placing information online does not ensure its control, and some safeguards for the data subject shall be ensured. In this regard, the limited administrative capacity of the authority imposing this obligation (e.g., lack of human resources) "cannot in any event constitute a legitimate ground justifying interference with the fundamental rights guaranteed by the Charter" (para 89). Therefore, for the Court, placing that kind and extent of information online does not pass the test of necessity.

Although passing the test of necessity is *a conditio sine qua non* to pass the overall test of proportionality, the court engages also in the last step of analysis, namely **proportionality *stricto sensu***. This step consists of assessing the seriousness of the interference to the rights of privacy and data protection, against the importance of the objectives of preventing conflicts of interest and corruption in the public sector (para 106). Notably, the Court notes that this balancing is not necessarily the same for all the Member States (para 110), as some might prioritise the need to fight corruption. Furthermore, the balancing shall take into, *inter alia*, the sensitivity of the data to be shared, their nature, the methods of collection and the number of persons having access to them (para 99), as well as account should be given to the importance of the duties carried out by the declarant (para 111) and the presence of safeguards against the risks of abuse of such DPI (para 113). For the Court, while considering the extent of the declarant's decision-making power, and provided that the principle of data minimisation is observed, the publication of such DPI may be justified by the benefits provided. In particular, this would strengthen the safeguards for probity and impartiality of public officials, such transparency, and aid the prevention of conflicts of interest and combating of corruption (para 115).

Overall, the Court interprets Article 6(1) and Article 6(3) GDPR as precluding national legislation that requires any head of an establishment receiving public funds to publish the DPI online, as envisaged by the Lithuanian law (para 116). Notably, it is the publication – online – of the information, as well as the generalised duty to any recipient of public funding, without consideration of their position in the public administration, which made the Court rule in this sense.

Regarding the second question, the analysis of the Court focuses on certain data, which although not being inherently 'sensitive', as defined in Art. 9 GDPR, have the potential of revealing sensitive information, such as sexual orientation. In this regard, the Court considered how name-specific data relating to the spouse, cohabitee or partner of the

declarant have the potential to reveal the sex life or sexual orientation of the latter and of his partner (para 119). In order to obtain the revelation, the Court refers to an “intellectual operation involving comparison or deduction” (para 120) as a sufficient condition for extending to personal data, which are not inherently sensitive, the special regime of protection envisaged for the protection of sensitive data.

Unfortunately, the Court does not discuss any further how this “intellectual operation involving comparison or deduction” should be conducted, whether certain criteria should be considered or whether it could be merely – and legitimately – based on stereotypes and common sense. Indeed, the Court grounds its reasoning on the need to ensure a coherent reading of the provisions regarding sensitive data, as well as ensuring a high level of data protection, especially with regard to certain aspects of private life (para 125-126).

Conclusion

This judgement answers two questions concerning the balancing of the rights of privacy and data protection with other public interests. In both cases, the Court stresses how ‘context’ will be the determining factor in striking the right balance. Yet, as the Court points out more than once, the elements of fact and law, that need to be taken into account, are specific to the case under consideration and affected by the legal system of the Member State concerned (para 86, 110).

Therefore, when considering how much emphasis is appropriate to give to this judgement, it should be kept in mind that the balancing stroke in this case is context specific to the factual and legal elements present in that Member State. This observation allows to say that, in the first question, the balancing between privacy, data protection and transparency is influenced by the Lithuanian administrative (legal and factual) setting and, therefore, not immediately, or necessarily applicable to other cases across the EU. For instance, other Member States may adopt a more aggressive anti-corruption policy, that would tighten transparency measures and – legitimately – limit the rights to privacy and data protection, as long as the ‘essence’ of these rights is not undermined.

Similar observations are applicable also to the answer given to the second question. The Court adopts a contextual approach, without making explicit the specific criteria for the determination of potentially sensitive personal data. Alternatively to a purely contextual approach, the Court should have used a more nuanced approach, that would have included elements of the purpose-based approach. Specifically, the Court should have considered that the administrative authority concerned did not intend, neither directly nor indirectly, to obtain information regarding the sexual orientation of the person subject to the transparency obligations. Moreover, the Court does not provide a taxonomy of

personal data, either concerning the same data subject or third parties, that combined among them would reveal sensitive information. The Court leaves this assessment on a case-by-case basis, and by doing this undermines legal certainty.

Although, the Court's intention, in consistent with previous [case law](#), is to ensure a high level of privacy and data protection, this approach does not promote a uniform interpretation of the law across EU Member States as well as does not ensure legal certainty to data controllers.