BCLP. Client Intelligent

Insights

DON'T ASK YOUR DPO TO SET THEIR OWN HOMEWORK AND MARK IT TOO!

CJEU RULING ON GDPR AND CONFLICTS

Feb 24, 2023

The recent CJEU decision in *X-FAB* (Case C-453/21) provides guidance on how to determine whether a conflict of interest could arise for your Data Protection Officer ("**DPO**") and how to avoid this. It also confirms the approach to potential incompatibility between (a) national laws providing enhanced job security for DPOs and (b) the objectives underlying the DPO function in the EU General Data Protection Regulation (2016/679) (the "**GDPR**"), especially where the DPO wears other "hats" within the organization. The decision is not binding in the UK but is still of relevance because substantially the same DPO framework applies under the UK GDPR.

In *X-FAB* an individual (FC) had been both works council chair and DPO since 2015. In 2017, at the request of the state data protection authority, X-FAB dismissed FC as DPO on the grounds that this was incompatible with the role of works council chair due to a potential conflict of interest. FC claimed that the dismissal was void due to protective employment provisions under German law. The matter was ultimately referred to the CJEU for a decision on a point of law.

The two main questions were:

1. How should a potential conflict of interest be assessed when it comes to the DPO function and any other tasks and responsibilities assigned?

2. If national law preventing the dismissal of DPOs is stricter than the GDPR's measures, is that incompatible with EU law or, more specifically, the GDPR?

CONFLICTS OF INTEREST

A DPO's mandatory tasks include monitoring the organization's compliance with the GDPR, the assignment of responsibilities, awareness-raising and training of staff, together with related audits (Article 39(1) GDPR). At the same time, Article 38(6) GDPR acknowledges that the person formally appointed as a DPO may fulfil other (non-DPO) tasks and duties, provided that the organization appointing the DPO ensures that any such other tasks and duties do not result in a conflict of

interest. The CJEU recalled that this provision aims to ensure the independence of a DPO, and thus guarantee the objectives of data protection. There is no fundamental incompatibility arising from assigning both DPO and non-DPO tasks, the Court noted.

The words "conflict of interests" should be given their everyday meaning said the Court, noting that "*the DPO cannot be entrusted with performing tasks or duties which **could** impair the execution of the functions performed by the DPO*" [emphasis added]. "Could" appears to give a cautious margin to the potential for a conflict of interest.

The CJEU held that determining the existence of a conflict of interest must be carried out "*case by case, on the basis of an assessment of all the relevant circumstances, in particular the organizational structure … and in the light of all the applicable rules, including any policies of the [organization]".*

As a more practical illustration, DPOs cannot be entrusted with tasks or duties which would result in them "***determining** the objectives and methods of processing personal data on the part of the controller or processor…Under [data protection law] the **review** of those objectives and methods must be carried out independently by the DPO*" [emphasis added]. In other words, DPOs cannot be put in a position where they are marking their own homework. The distinction is not always obvious, particularly because of the increasing interdependence of regulatory compliance and business operations.

DISMISSING A DPO

On this question, the answer is no - the GDPR does not prevent enhanced protection for DPOs being enacted at national law level, per se. The Court cited its decision in *Leistritz* from June 2022 (Case C-534/20), which considered whether the GDPR (Article 38(3)) precluded a member state from passing legislation which was more protective of a DPO's employment status, i.e. making it more difficult than under the GDPR to dismiss a DPO. Article 38(3) of the GDPR states *"[a DPO] shall not be dismissed or penalised by the [organization] for performing his tasks"*. The CJEU held that member states, such as Germany, are free to lay down more protective provisions provided that these remain compatible with EU law and do not undermine the achievement of the GDPR's objectives, particularly the functional independence of the DPO. In *Leistritz*, an unacceptable example given was of national law operating so as to prevent an organization from dismissing a DPO who no longer possessed the professional qualities required to perform their tasks, or who did not perform those tasks in accordance with the GDPR's requirements.

In *X-FAB*, noting that it was for the German national court to satisfy itself that the specific protective provisions are compatible with EU law and the GDPR, the CJEU indicated that a national law which prevented the dismissal of a DPO who was unable to carry out their role in an independent manner because of a conflict of interest would not be compatible with the GDPR.

POSSIBLE NEXT STEPS

The EDPB has announced it has selected the designation and position of the DPO role as the focus for its next coordinated pan-EU enforcement action. For that reason, as well as the two CJEU decisions discussed above, this could be a suitable point for organizations to re-evaluate their DPO function.

It is possible for jobs and roles to evolve over time. If you have appointed a formal Article 37 DPO, is that same person now also entrusted with other tasks or duties which could impair the performance of their DPO obligations? Are you placing them in the untenable position of "marking their own homework" and leaving your organization at risk of missing its data governance obligations? Are there clarifications which can be provided to delineate your organization's expectations? How best can any necessary adjustments be addressed in a manner which complies with employment law, not just the GDPR?

Even for companies which are not required to appoint a formal DPO, considering how to ensure the independence of your data privacy function, and avoiding combining incompatible responsibilities, provides a useful blueprint for effectiveness.

If you would like to discuss any of the matters raised in this briefing, please contact any of the authors or your usual BCLP lawyer.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Kate Brimsted

London

kate.brimsted@bclplaw.com
+44 (0) 20 3400 3207

Pierre-Emmanuel Froge

Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483