



16 October 2024

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data
protection authority

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) Autumn Conference

Speech by;

Wojciech Wiewiórowski
European Data Protection Supervisor

Good morning, ladies and gentlemen, Dear data protection professionals,

First of all, I would like to thank you for the invitation. It is a pleasure for me to take part in this conference and to share my vision, as European Data Protection Supervisor (EDPS), on the function of the Data Protection Officer (DPO) and on the future.

The EDPS is an independent supervisory authority responsible for ensuring that the Union institutions, offices, bodies and agencies (EUIs) comply with their data protection obligations. The EDPS is currently supervising 75 EUIs spread out all over the 27 EU Member States.

The main tasks of the EDPS as a supervisory authority are the same as those of the national supervisory authorities, ranging from monitoring and advising activities to enforcement and cooperation.

The EU public administration is subject to Regulation 2018/1725 – which we call the EUDPR, the “GDPR for EUIs”.

The EUDPR, obliges the EUIs to appoint a Data protection officer. The DPO function has a long tradition within the EUIs, since DPOs existed even before the establishment of the EDPS in 2004.

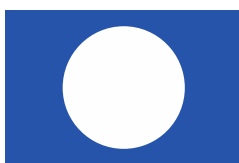
DPOs have proven to be a success not only in their work in the EUIs, but also in the creation of a DPO network. I will come back to that later.

The EUDPR mirrors largely the GDPR on the **designation** and **position** of the DPO, but it provides more specific rules than the GDPR on the mandate of the DPO, which can be between 3 and 5 years, and can be renewed. The EUDPR also sets out conditions for their dismissal, which requires the prior consent of the EDPS.

I would also like to stress that the list of DPO **tasks** in the EUDPR is more detailed than in the GDPR. In particular, the DPO should:

- ensure in an independent manner the internal application of the EUDPR;
- ensure that data subjects are informed of their rights and obligations and that these rights are not adversely affected by processing operations;
- respond to EDPS requests, and consult with the EDPS, and
- investigate data protection matters.

This shows that the DPO in EUIs not only has to *advise* their institution on the application of the rules, but is also obliged to *ensure*, independently, that the EUDPR is applied.



The EDPS is also a member of the European Data Protection Board (EDPB). As such, in 2023, we participated in the Coordinated Enforcement Framework action of the EDPB on the position of the DPO and carried out a survey on the matter among all EULs in 2023.

Today, I would like to share with you 4 of the most common challenges faced by 'our' DPOs, as highlighted by a recent EDPS survey.

The lack of resources to fulfil their tasks is an issue for almost half of the survey respondents.

According to the survey results, less than one third of the survey respondents are full-time DPOs. Moreover, less than half of them have a deputy, and a vast majority do not have anyone or have only a part time resource to assist them. This translates to lack of time to perform DPO duties, but also to attend training activities.

DPOs are a part of the institution and yet must remain independent from it in the performance of their duties. DPOs might sometimes be inclined to accept certain compromises when dealing with controllers in high positions, or fear that their stance could influence the renewal of their contract or their career progression.

Less than 10% of the DPOs report that they receive instructions from their management. Nevertheless, a very small number reported that they have been penalised for performing their tasks.

The requirement to act in an independent manner is closely linked to the absence of conflict of interests.

The survey report highlights that such conflicts may arise, notably when DPOs are asked to take additional tasks that should normally be performed by the data controller.

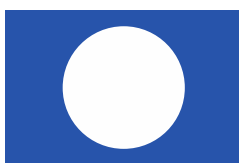
According to the survey results, the involvement of DPOs in decisions with data protection implications is high within EULs, with a large majority reporting that they are involved in virtually all data protection issues, that their opinions are followed in most cases and that the reasons for not following their advice, where applicable, are documented.

I will of course follow up on these insights in order to improve the DPOs' positions.

To me, and to the EDPS as an organisation, the role of the DPO is essential. DPOs are our main interlocutors and act as our contact point with the institutions that we supervise. We have a privileged relationship with them - since they are a relatively small group of people, we know them all and have regular contacts with them.

The EDPS develops this collaboration on 3 main areas:

DPOs can consult the EDPS on any data protection matter, which results in a supervisory opinion. We also regularly publish guidance on a wide range of data protection-related topics.



When the EDPS handles complaints or exercises corrective powers, the DPO can be seen as a strategic partner who can help determine the well-targeted application of a particular data protection measure.

As already mentioned, the EDPS organises biannual meetings with the DPOs of the EUs. These meetings are an important opportunity to exchange practices, provide further guidance and clarifications.

I would like to end my intervention with a few words on the major challenge that we all face these days: the ever-increasing use of Artificial Intelligence, and more specifically, the AI Act and its interaction with the data protection framework.

Well, we would probably all agree that data protection and AI are heavily interlinked. My message: Data protection and privacy will not merge, nor will they disperse into Artificial Intelligence.

I am here today to defend data protection and privacy against the risk of diluting them into the AI hype. In fact, this could only mean dangerously weakening these fundamental rights; the two must remain separate.

However, I am not naive, and you are not a naive community either. Of course, Artificial Intelligence is fuelled by data, much data that some operators refuse to recognise as 'personal' because (they claim) these data have been aggregated or anonymised. Artificial intelligence and data protection are different, and so are the legislative frameworks related to them.

Compliance with data protection and privacy rules is the essential prerequisite to put people at the centre, and ahead of technology. That is why, we must work together to defend the identity of data protection to protect humanity. But how do we do that?

You may know that, in addition to its role as data protection supervisory authority under the EUDPR, the EDPS is the competent authority and market surveillance authority for AI systems put into service or used by EUs under the AI Act.

In this role, and *not* in our role as data protection supervisory authority, we have developed a strategy for the use of AI systems in the EUs. The plan includes a proposal that EUs appoint an 'AI Act Correspondent' to facilitate compliance with the obligations stemming from the AI Act.

The role of the AI Act Correspondent is not the same as that of a DPO and it cannot replace that function.

Nevertheless, it is clear to me that DPOs must in any case be part of the discussions whenever their EU intends to develop or to use AI systems that process personal data.

This proves, if proof was necessary, the importance of the DPO function to face the challenges of today and of tomorrow. Thank you for your attention.

