Bonn, Bucharest, Dublin, Lisbon, Madrid, Milan, Paris, The Hague, Vienna, Warsaw

Is the DPO the right person to be the AI Officer?

CEDPO AI and Data Working Group
Micro-Insights Series
July 2024

Authors:
Marc Bellon
Lionel Capel
Ernst-Oliver Wilhelm
Maria Moloney

Contact information:
https://cedpo.eu
info@cedpo.eu

About the Micro-Insights Series

The Micro-Insights Series is a publishing initiative by the CEDPO AI and Data Working Group. It will provide digestible, definitive, short-form papers on key areas of interest at the intersection between data and artificial intelligence. With a practical focus, keeping one eye on explaining complex topics and the other on implementation, it will outline the significance of key areas and advise practitioners on impact, and next steps. With the EU Artificial Intelligence Act (the 'AI Act') coming into law in 2024, the scene is now set for all practitioners, and it is possible to discuss the regulation of data and AI with much greater clarity.

The Micro-Insights Series will follow the evolution of AI and data over the coming years, and as the clock winds down on the crucial implementation period for the AI Act, and as AI technologies evolve in ever-more novel and unexpected ways, the Series will respond with up-to-date, authoritative guidance on the core areas of concern.

Amongst others, the series will include papers on:

- Regulation of General-Purpose Artificial Intelligence under the AI Act
- Explaining the AI Pact.
- Educating practitioners on how to conduct Fundamental Rights Impact Assessments under the AI Act.
- Outlining the role that data protection regulators will have in AI regulation.
- Examining whether or not the data protection officer is the right person to be the AI officer.
- The lawful basis for using training data in machine learning.
- Readiness toolkit for the AI Act.

CEDPO
CONFEDERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS

Table of Contents

1. The Evolving Role of the Data Protection Officer

The role of the European Data Protection Officer (DPO) for the last six years, since the advent of the General Data Protection Regulation (GDPR), has evolved and expanded in line with the growing use of technology and data within organisations. The processing of both data and personal data has grown exponentially in the European Union (EU) and also globally. As a result, many countries are beginning to follow in the footsteps of the EU by introducing their own versions of data protection legislation.

Even though the GDPR is six years old, it includes provisions on automated decision-making. Now in the age of Artificial Intelligence (AI), these provisions empower DPOs to regulate the use of AI in processing personal data. The GDPR grants data subjects the right to object to automated decision making, especially those decisions based solely on profiling, if such decisions have significant legal or personal consequences. DPOs must, thus, ensure that data subjects have the possibility to request either human intervention or some other way to challenge automated decisions. On top of this, the DPO also has the responsibility of carrying out routine checks to make sure that any automated systems are working as intended.

Under the EU AI Act, many types of automated decision-making systems fall within the category of high-risk systems. When such systems process personal data, DPOs need to ensure Data Protection Impact Assessments (DPIAs) are carried out and appropriate safeguards are introduced where necessary before the deployment of such systems should take place.

On December 7th 2023, the European Court of Justice (ECJ) issued a landmark ruling against the German credit scoring agency Schufa AG Holding ("SHUFA"), which strengthened individual rights around automated credit scoring. The court held that creating a credit score constituted an "automated individual decision" pursuant to article 22 of the EU GDPR. This decision was significant because it granted data subjects the right to object to such scores and request human intervention in the score creation process. While credit scoring is still permitted, the ECJ emphasised the need for measures to be put in place to safeguard fairness and individual rights.

From a more general perspective, the ECJ ruling has the potential to affect service providers who employ automated processes for generating risk-based scores or other outputs, especially if those outputs play a pivotal role in decisions significantly affecting data subjects. Based on this assessment, the judgement clearly strengthens the DPO's position around their obligations to protect personal data used in any type of automated decision-making process. This is perhaps where the idea of the DPO assuming the role of AI officer within organisations originated. This idea, however, is more complex upon reflection and is discussed below.

2. Is the DPO Best Placed to Become the AI Officer?

Regardless of whether DPOs take full ownership of AI compliance within an organisation, clearly they must be part of the discussion whenever AI systems process personal data. Adding to this, there is currently no universally accepted understanding of the term 'AI Officer' and, in contrast to the DPO, whose designation, and responsibilities are defined in articles 37-39 of the GDPR, the AI Act does not define the role of an AI Officer, nor does it specifically mandate the appointment of an AI Officer.

Appointing an AI Officer or perhaps a *Chief* AI Officer is a likely step for some organisations in the near future. With the inclusion of risk management and compliance in this role, and depending on the nature of the job specification, there could be potential limitations to the AI officer's effectiveness. An AI Officer focused solely on risk and compliance might miss the potential of AI for transformation, efficiency gains, and new business opportunities. Thus, promoting the DPO to this role might present challenges, as discussed below.

- Assigning a DPO decision-making powers over AI governance may create a conflict of interest under Article 38 of the GDPR. This article prohibits situations where the same individual is responsible for both implementing data processing activities and ensuring compliance with data protection rules.
- Furthermore, assigning the AI Officer role to the DPO could compromise the DPO's independence, a crucial aspect of the DPO position as outlined by the GDPR. Organisations likely need clear lines of authority and distinct roles for AI implementation and data protection oversight.

Alternatively, some organisations could create an 'AI Risk Officer' role. This role could focus on risk management and compliance, ensuring AI systems (AIS) adhere to the risk-based approach outlined in the AI Act. The AI Risk Officer might also consider ethical principles to promote trustworthy AI. While this role shares some overlap with the DPO's responsibilities, particularly in data protection aspects, it would not encompass the full scope of an AI Officer role that is focused on driving AI transformation and opportunity. Consider the following three scenarios:

2.1 AI Officer in small and medium organisations

Due to a lack of resources and/or employees with the requisite skills, DPOs become responsible for both data protection and AI compliance. In this scenario, it is unlikely that such a DPO could oversee a large data protection and AI compliance function in parallel. The likely use cases for AI within such organisations would be the governance of chatbots and tools such as ChatGPT or Copilot as well as oversight of some suppliers' AIS. Such a DPO would, therefore, need to develop their skills in generative AI governance in order to take on these new responsibilities.

2.2 AI Officer in large organisations

The parallel deployment of data protection and AI compliance seems more likely in larger organisations. Such use cases might include:

- the use of AI in software packages or business solutions.
- creating in-house AI systems with or without the support of external partners. The development and deployment of such systems would, however, result in the organisation being classified as either a developer or a deployer of AI systems under the EU AI Act. This would result in the company needing to comply with all the regulatory consequences that this brings.

Although AI regulatory compliance might not fall directly under the DPO's purview, their expertise would be crucial in areas that significantly overlap with GDPR requirements. This would include data protection, bias detection (especially in high-risk AI systems), and assessing mandatory human oversight for both system operations and fundamental rights considerations.

2.3 AI Officer in AI Developer and Deployer Organisations

The EU AI Act necessitates distinct roles for developers and deployers of AI systems. Both entities have distinct responsibilities under the Act to ensure the safe and responsible use of AI. DPOs in these organisations will require specific and specialised knowledge of their internal AI systems if they are to fully understand and keep abreast of the functions of these systems that are so prone to change and adaptation (learning) in the face of new requirements and deployments.

3. Conclusion

In summary, DPOs might potentially take on the role of an AI Officer in certain scenarios, as there is a significant overlap in the ethical, legal, and governance aspects of these two roles. However, clearly defining the scope, duties, and expectations of the AI Officer role can help determine whether the DPO could effectively transition into this new position or even incorporate it into their existing data protection role.

No matter the organisational size or scenario, DPOs should expect increased responsibilities – at the very least in ensuring AI systems comply with data protection requirements.

From a more general perspective, the possible merging of DPO and AI Officer roles could be signalling a significant shift taking place in the field of governance, risk, and compliance (GRC). This shift might necessitate the creation of a new leadership position, possibly something along the lines of Chief Data Compliance Officer, who would oversee compliance across all data and digital projects and organisational systems.