CEDPO
CONFEDERATION OF EUROPEAN
DATA PROTECTION ORGANISATIONS

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

CEDPO Opinion on the potential impact of the EU's proposed Artificial Intelligence Act (AI Act) on the role of the data protection officer

Contact information:

https://cedpo.eu

info@cedpo.eu

1. Introductory Context

Recital 45(a) of the proposed draft AI Act broadly outlines the intended way in which the GDPR and the AI Act will interact with each other: “The right to privacy and to data protection must be guaranteed throughout the entire lifecycle of the AI system. In this regard, the principles of data minimisation and data protection by design and by default, as set out in Union data protection laws, are essential when the processing of data involves significant risks to the fundamental rights of individuals. Providers and Users of AI systems should implement state-of-the-art technical and organisational measures in order to protect those rights. Such measures should include not only anonymisation and encryption, but also the use of increasingly available technology that permits algorithms to be brought to the data and allow valuable insights to be derived without the transmission between parties or unnecessary copying of the raw or structured data themselves.”

This opinion paper seeks to draw out the significance of the above recital, and to discuss the critical points at which the AI Act and the GDPR will interact, with particular emphasis on how this new more complex legislative environment will potentially impact the role of the data protection officer.

In general terms, CEDPO has some concerns about the numerous legislative initiatives that the EU is enacting under the umbrella of its Data Strategy, and, specifically, how these new laws will interface with the role and responsibilities of the data protection officer, a role which already has a busy and demanding brief under the tenets of the GDPR. Aside from the AI Act, the following legislation is also being developed by the EU: The Data Act; the Data Governance Act; the Digital Markets Act; the Digital Services Act; as well as the revised ePrivacy Regulation.

From CEDPO’s perspective, it is a central contention that the role of the DPO should be supported and not burdened by the enactment of multiple pieces of complex legislation in the digital space. With these concerns in mind, this paper will look at the significance of the AI Act for the DPO. Although the AI Act does make some significant references to the GDPR and data protection, most notably in the above-referred Recital 45, and in Art. 10, which outlines some of the data obligations placed on providers of high-risk AI systems, **CEDPO is of the view that, where personal data and AI overlap, important clarifications remain to be made on the practical manner in which both Acts will work together.**

It is accepted by CEDPO that Art. 22 of the GDPR already partially clarifies the obligations that arise from AI or machine-learning technologies processing personal data via automated decision making, however, CEDPO believes that the new, extensive requirements introduced by the AI Act, will significantly outstrip any existing clarity offered by Art. 22. As such, this paper seeks to explore these legislative grey zones, where new dependencies will be created between the GDPR and the AI Act, and from the perspective of the DPO, raise the pertinent questions that will need to be addressed by the EU policymakers in the coming months.

2. How will the key roles under the AI Act and the GDPR align with each other?

It will be very important for clarity to be achieved on how the existing responsibilities of Controllers, Processors and Joint Controllers, as outlined in the GDPR, map onto the key roles identified in the AI Act, namely Providers, Users, Importers and Distributors.

On 19 February 2020 the EU Commission adopted its White Paper on *Artificial Intelligence - A European approach to excellence and trust* (the "White Paper on AI") whose purpose was to set out the policy options to achieve the twin objectives of promoting the uptake of AI and of addressing the risks associated with certain uses of this emerging technology.

In this report, the Commission expressly recognized that *"Europe's current and future sustainable economic growth and societal well-being increasingly draws on value created by data. AI is one of the most important applications of the data economy. Simply put, AI is a collection of technologies that combine data, algorithms and computing power. Advances in computing and the increasing availability of data are therefore key drivers of the current upsurge of AI".*

The strong connection between data (either personal or non-personal) and AI systems is reflected also in the draft AI Act, which expressly sets out that *"Union law on the protection of personal data, privacy and the confidentiality of communications applies to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation shall not affect Regulations (EU) 2016/679 (**the "GDPR"**), (EU) 2018/1725, Directives2002/58/EC and (EU) 2016/680".*

Among the various aspects of interaction between the GDPR and the AI Act, one of the most evident is that of the potential overlapping of obligations and responsibilities between the various players that are required to comply with the respective regulations. In particular, Controllers, Joint Controllers, Processors on the one hand, and Providers, Users, Importers and Distributors on the other. As AI usually involves processing personal data in several different phases or for several different purposes, **it is possible that a single Provider, User, Importer or Distributor may be a Controller or Joint Controller for some phases or purposes, and a Processor for others**.

Focusing in particular on key roles under the AI Act, the regulatory framework provided by the regulation is complex and onerous and is addressed to all parties involved in the development and further commercialization of High-Risk AI systems (the "**HRAI Systems**"). Although most of the obligations under the AI Act are intended for Providers, specific obligations are also placed on other roles, such as Users, Importers and Distributors, whose role is outlined in the regulation itself.

As far as Providers are concerned, the AI Act provides for a set of "mandatory requirements" that they must adhere to as from the design and development of the HRAI system, before it is placed on the market or deployed into service, and also beyond, during its entire life-cycle. Certainly, many of these requirements will necessarily involve the processing of personal data, and consequently the possible simultaneous subjection to **dual obligations** under the GDPR and the AI Act.

We refer, in particular, to the following:

- **Risk management system**: The Provider is required to implement, in a documented manner, a system to ensure compliance with the AI Act, and to identify and analyse the known and the reasonably foreseeable risks that the HRAI system can pose to the fundamental rights of natural persons, estimate them, and take appropriate measures. The specific risk assessment carried out for these purposes might result in duplication and **overlap with the risk analysis** that the Provider or User in their capacity as Controller must carry out under Arts 24, 25, 32, and 35 of the GDPR.

- **Data governance**: Under Art. 10 of the AI Act, the datasets used by the Provider in training, validation and testing are subject to appropriate data governance standards and must meet high requirements for relevance, representativeness, correctness, and completeness in order to limit the possibility of harmful and discriminatory bias.

  The principles of **data minimisation** and of **data protection by design and by default**, as referred to respectively, in Art. 5(1), point (c) and in Art. 25 of the GDPR shall be applied when developing and using HRAI systems and during the entire lifecycle of those systems.

  Compliance with this provision will entail for the Provider, or for the User (where the Provider does not have access to the data and the data is held exclusively by the User), certain specific obligations under the GDPR.

  There is a concern over the fact that this rule refers to only **one of the principles** in Art. 5 (i.e., data minimization), while others which would seem equally applicable (i.e., data accuracy, purpose limitation, etc.) are not referenced. Additionally, there is possible **duplication of responsibility** for the User who might be required to comply with this rule both under a contract with the Provider as well as under the GDPR, acting as Controller.

- **Record keeping**: Providers, assuming the HRAI system is within their control, must ensure the verifiability and traceability of the decisions and processes put in place by HRAI systems (Art. 12 AI Act). This is to be achieved by providing mechanisms for automatic logging, in order to ensure and demonstrate compliance with the AI Act. This relates to ex-post audits of any reasonably foreseeable malfunctions or misuses of the system, or for ensuring and monitoring for the proper functioning of the system throughout its entire lifecycle; the logs shall be kept for a period that is appropriate in light of the intended purpose of the HRAI system and applicable legal obligations under Union or national law.

  The retention of logs - by the Provider or the User, as the case may be - will have to be in line with Art. 5(1)(e) of the GDPR regarding the Controller's compliance with the storage limitation principle. It would be instructive if a better explanation would be tendered of what "retained for a period appropriate in light of the intended purpose of the high-risk AI system" means. This has particular relevance in light of compliance with Art. 11 of the GDPR, according to which: “If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation”.

  Again, any Joint Controllers’ Agreements, or Data Processing Agreements between Providers and Users will need to carefully regulate the fate of personal data contained in the logs once the contractual relationship is terminated (i.e., shall the User (Controller) be entitled to ask the Provider (Processor) to cancel or anonymize the logs, containing for instance the input data, once the relationship has ended?).

- **Appointment of authorised representatives**: Prior to making their systems available on the Union market, Providers established outside the Union shall, by written mandate, appoint an authorised representative which is established in the Union (Art. 25 AI Act). Such provision might interfere with the duty laid down by the GDPR on the Controller or Processor to designate a representative in the Union where Art. 3(2) applies. A clarification on the possibility to appoint the same person for both purposes might make the duty less burdensome on Providers.

With regard specifically to Users, in addition to those mentioned above, several provisions of the AI Act impose on them typical obligations of the Controller and/or Processor under the GDPR, namely:

- **Appointment of persons in charge of processing:** Users of high-risk AI systems shall ensure that individuals assigned to provide human oversight of high-risk AI systems are competent, properly qualified and trained and have the necessary resources in order to ensure the effective supervision of the system in accordance with the Art. 14 of the AI Act.

- **Relevance of data**: Users shall ensure that input data is relevant in view of the intended purpose of the high-risk AI system, echoing principles of the GDPR on fairness, purpose limitation, minimization and accuracy.

- Where applicable, Users of HRAI systems shall carry out **a data protection impact assessment** under the GDPR having regard to the technical characteristics of the system, the specific use and the specific context in which the AI system is intended to operate.

- Users of HRAI systems, which make decisions or assist in making decisions related to natural persons, shall **inform the natural persons** that they are subject to the use of high-risk AI systems. Again, Users of HRAI systems that generate, on the basis of limited human input, complex text content, such as news articles, opinion articles, novels, scripts, and scientific articles, shall disclose that the text content has been artificially generated or manipulated, including to the natural persons who are exposed to the content, each time they are exposed, in a clear and intelligible manner.

  Such transparency duties **will have to be coordinated** with the Controller's duty to provide information under Arts. 13 or 14 of the GDPR, as applicable.

With reference to Importers and Distributors, the AI Act does not seem to envisage any specific involvement of these individuals in activities that entail, per se, the processing of personal data and, consequently, the assumption of the roles of Controller or Processor under the GDPR.

In general terms, CEDPO would welcome appropriate clarification on the ways in which defined roles under the GDPR and under the AI Act **will interact with each other** in real-life data processing scenarios.

3. How will risk assessments under the GDPR and the AI Act be managed from an operational perspective?

A key overlap between the AI Act and the GDPR is the obligation to manage the risks to individuals that may be affected by the convergence of data processing and AI systems. Under the GDPR, this is addressed through the principles of data protection by design and by default, and in particular by conducting a data protection impact assessment (DPIA); while under the AI Act, conformance assessments and risk management obligations exist, as well as a reference to the use of DPIAs "where applicable".

The concern with AI systems arises where these systems have direct or indirect impact on data subjects i.e., where they are directly processing personal data with direct impact on data subjects (e.g. facial recognition, credit scoring, immigration checks), or where their processing has an impact on the environment in which data subjects interact (e.g. autonomous driving systems, medical diagnostic systems).

The GDPR is clear that a DPIA is required where automated decision-making or profiling is taking place, and this accounts for a large number of AI systems in use, and certainly all those with an impact on natural persons. And even in AI use cases where the criteria of automated decision-making or profiling are not fully applicable, by matching or combining datasets and applying new technological solutions relevant AI use cases will inevitably require a DPIA according to the EDPB guidance 'Guidelines on Data Protection Impact Assessment (DPIA)'.

The AI Act, on the other hand, refers to such a requirement only under Art. 29 (6), and then only "where applicable". Nevertheless, it is clear that a DPIA is likely "applicable" in a **large proportion** of AI uses-cases.

In such instances, **the burden on those advising on how the DPIA is conducted**, (most likely DPOs) is likely to be considerably larger than in typical circumstances. This is for a number of reasons:

- *Art 29 (6) states that "Users of high-risk AI systems shall use the information provided under Art. 13 to comply with their obligation to carry out a [DPIA]."* Art. 13 is an obligation on the provider of the AI system to detail certain information, the interpretation of which in a local processing context will require considerable insight on the part of the DPO. CEDPO notes that there is no complementary obligation on the part of the AI system provider to provide such information as might be necessary to otherwise complete a DPIA under the GDPR. This imbalance risks imposing additional burdens on DPOs that could compromise the DPIA process.

- It is not clear whether the AI Act's obligation to create and maintain a risk management system in respect of the deployment of an AI system is satisfied by a DPIA-type risk analysis (or vice versa), and so, in the absence of guidance, potentially unnecessary duplication of effort is likely to take place.

- In instances where the User is also the Provider, all the obligations under Chapter 3 of the AI Act also apply, and the potential is that the bulk of these requirements shall fall to the DPO.

4. How will the AI Act affect the role of data protection officer?

CEDPO has concerns about the role which DPOs will be expected to play in contexts where personal data and relevant AI applications overlap. For instance, will DPOs be expected to become **increasingly proficient in more technical AI software considerations**, and if they do so, will this **compromise their statutory independence** and/or expose them to challenges **beyond their expertise**?

CEDPO is of the view that the role of the data protection officer within an organisation should, in line with its strict legislative brief, **remain focused on advising on compliance with the GDPR and other relevant Union or Member State data protection provisions**.

The role of the DPO has a clear basis in legislation at Arts. 37-39 of the GDPR. The proposed text of the AI Act, however, is silent on a corresponding role that might **oversee its compliance and regulatory requirements**. CEDPO would welcome further clarity on how organisations are proposed to resource the regulatory obligations imposed by the proposed AI Act, in a manner similar to the prescription of the DPO role in the GDPR.

Similarly, based on the sector/size/activities of an organisation, it would be particularly helpful if it were mandated under what circumstances the equivalent of a DPO should be appointed under the auspices of the AI Act. CEDPO notes recent calls from industry professionals for the establishment of a position of **AI Officer** under the proposed AI Act and would welcome consideration of this as a means for addressing concerns outlined above. This would present an opportunity to **distinguish roles** in respect of technical knowledge of data protection law and AI regulation law **(DPO)** on the one side, and technical knowledge of AI systems and broader regulatory context beyond data protection laws **(AI Officer)** on the other side.

Such clarity is now required in order to avoid a foreseeable risk to the role of the DPO, where he/she may be expected **to take on responsibility** for activities related to AI within an organisation, which **infringe on the independence of the role** and create an inherent **conflict of interest** (e.g., an executive function related to AI systems and/or defining processing activities related to AI systems). This could result in a potential breach of a Controller or Processor obligation under Art. 38 (6) GDPR not to assign tasks and duties to a DPO that would result in a conflict of interest. CEDPO is cognisant of recent decisions of data protection authorities (such as issued by the Berlin DPA and Belgian DPA) which imposed fines on controllers for breaches of Art. 38 (6).

The highly undesirable outcome, from CEDPO's perspective, would **see DPOs managing significant aspects of both regulations**, meaning that he/she would **perhaps become responsible for AI Act requirements even when they do not concern personal data**.

The alternative solution, having the DPO managing the AI Act part that concerns only personal data, and the AI Officer the remaining part, brings also some difficulties. Indeed, having **two persons working on the compliance of a single act** could be a source of confusion, conflict, and repetition.

A potential positive outcome for DPOs, with respect to the enactment of the AI Act, could be achieved if the final regulation **were to govern the creation and use of derived (personal) data**.

Derived personal data is personal data that is extrapolated from existing datasets through the use of AI algorithms. Examples of this would be the use of AI to analyse CCTV images or GPS location data and, thereby, identify additional categories of personal data, such as, perhaps, historical location data or the sexual orientation of an individual.

An opportunity exists to require that those responsible for AI processing, whether Providers or Users, **provide clear identification and classification of such derived personal data**. Such a requirement would greatly assist the DPO's obligation to maintain accurate and up-to-date **records of processing activities**.

5. How will the respective data protection and artificial intelligence regulators interact?

It appears clear that the AI Act envisages the creation of stand-alone AI regulators in all Member States, in addition to existing regulatory bodies. How will investigation and enforcement action be conducted, where, for example, the **data protection regulator and the AI regulator both have a stake in the matter at hand?** Moreover, how will the regulatory bodies interact with the EU institutions?

One case of regulatory interaction, at least, seems to be clear: the European Data Protection Supervisor (EDPS) may impose administrative fines on Union institutions, agencies and bodies falling within the scope of the AI Act.

However, the picture with other relevant regulatory bodies is not so clear. The European Data Protection Board (EDPB) equivalent in the AI Act is the proposed European Artificial Intelligence Board (EAIB). However, the EAIB has no enforcement powers, even though the fines under the AI Act are potentially even greater than under the GDPR. The AI Act does not specify who shall be responsible for enforcing the fines and leaves it to every Member State to designate appropriate rules and legislation to implement the regulation.

Oversight and conformance under the AI Act is left to the Member States, which is a cause of concern as there could be considerable **divergence as to how the Act is governed/applied across Member States**. Furthermore, there is **no 'one-stop shop' equivalent** under the AI Act. The (EAIB) has no enforcement abilities; its brief is limited to streamlining the application of the Act across the Member States and assisting the EU Commission in its tasks. Ultimately, CEDPO has concerns that these issues could **hamper the ability of DPAs to coordinate effectively with their AI equivalent-regulators**.

6. How will data subject rights be protected in contexts where both the GDPR and the AI Act apply to the subject matter?

In general terms, CEDPO is of the view that the full and proper resolution of rights-based actions initiated under the GDPR are likely to become dependent on the proper functioning of the AI Act, once it becomes law. Especially, where the matters under consideration concern both data protection and AI, it is likely that the twin regulatory machinery will come into play. In such cases, CEDPO would wish to see that the justice of data protection claims is not jeopardised by any resulting dual regulatory regime that may result from data protection and AI regulators having common authority over the one matter.

Additionally, current drafts of the AI Act do not make it clear whether or not this legislation will be fundamentally rights-based in nature, as the GDPR is. In circumstances where two pieces of legislation are likely to become inextricably linked over time, but where one is significantly rights-based and the other is not, CEDPO would query **how rights initiated under the GDPR** will be **adequately resolved** through the likely, necessary interplay with the AI Act. In order for the GDPR to interact more harmoniously **with the AI Act**, it will be better if the latter Act is also framed with a **strong emphasis on rights**.

As complaint-handling is already a sensitive issue under the GDPR, with some supervisory authorities taking a number of years to resolve data protection complaints, CEDPO would be keen to understand how the **complaints process** will function once the AI Act is in law. In particular, where the relevant matter has significant **data protection** and **AI components**, will data subjects be expected/required to make separate submissions to separate regulators? If this is the case, the concern is that an already complex and strained resolution process will only become lengthier, with it becoming increasingly difficult for data subjects to achieve adequate justice. Certainty of process will be required and, in particular, it must be clarified if a **dual complaints-handling process** is envisaged, or, if instead, one authority will be nominated, with the other, perhaps playing the role of a notice party.

Additionally, the criteria for establishing **competency to handle complaints** will be a key consideration. It is likely that many complaints will involve significant, technical matters, which are more properly investigated by an AI regulator, and where a data protection regulator will struggle; conversely, where the matter involves precise matters of data protection law, a would-be AI regulator is likely to fall short, with only a data protection regulator holding the requisite expertise. CEDPO's hope is simply that a **manageable complaints process** would result from the inevitable interaction between the competent supervisory authorities.

There is also a risk of divergent approaches to rights from the differing regulators. For example, **differing approaches from the EDPB and EAIB** may occur on guidance on the same subjects. Moreover, any given AI regulator will have differing and competing priorities beyond data protection, whereas data protection regulators have only one priority. Also, if **lower thresholds** emerge from guidance-to-guidance DPOs may come under pressure from Boards who do not wish to apply the higher standard.

Even though the AI Act seeks to address risks to individuals, where protection of the rights of individuals is concerned, the GDPR is a more instructive example of how to protect rights. This is apparent when comparing GDPR Recital 1 (starting with 'fundamental rights') against Draft AI Act Recital 1 (starting with 'functioning of the internal market').

It would be very useful to include a provision in the AI Act spelling out how both Acts will interact on key matters, such as **protection of rights**. It is **not sufficient** to state that one text is 'without prejudice and complements' in the explanatory memorandum. An example of a stronger and clearer way forward can be found in the draft Data Act, Recital (7) and Art. 1(3).

CEDPO would also welcome clarity on what is expected of the DPO, in particular, in their attempts to successfully meet **data subject rights requests** in contexts where the GDPR and AI Act overlap.

19/12/2022

Contact information

Email: info@cedpo.eu / Website: www.cedpo.eu