CEDPO

CONFEDERATION OF EUROPEAN
DATA PROTECTION ORGANISATIONS

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

AI and Personal Data
A Guide for DPOs
“Frequently Asked Questions”

CEDPO AI Working Group
16 June 2023

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

CEDPO

CONFEDERATION OF EUROPEAN
DATA PROTECTION ORGANISATIONS

About this Guidance

This guidance has been prepared by the Confederation of European Data Protection Organization's AI and Data Working Group. It is aimed at data protection officers and answers, for them, the fundamental questions that will arise as their work inevitably intersects more and more with artificial intelligence and machine learning software.

Artificial intelligence and machine learning technologies are growing rapidly and exponentially, and although they do not always process personal data, when they do, it is often on a vast scale and level of complexity.

This introduces new risks for data subjects as well as new challenges for the DPO who, typically, may not necessarily have a computer science background, but will nonetheless be expected to analyse and understand the inner workings and implications of these technologies. DPOs have a twin challenge: they are faced with a steep learning curve, and in a dynamic area of technology that is evolving daily before their eyes.

Although there is an existing onus on DPOs to apply data protection principles to artificial intelligence, already a complex task, (and something which this guidance explains), new regulation is also on the horizon.

The EU's Artificial Intelligence Act is making its way through the EU legislative machinery, with an anticipated enactment date in 2024. Once in law, this Act will overlap with the GDPR in important ways, leading to additional obligations for DPOs. This guidance seeks to point out the junctures between these two major, and connected pillars of the EU's regulatory framework.

Companies and public bodies are moving fast to understand and implement artificial intelligence solutions to achieve all manner of efficiencies and opportunities for revenue growth. The DPO has no choice but to keep pace; technology will not wait. This guidance, therefore, represents a starting point for DPOs to begin navigating the increasingly critical and complex world of artificial intelligence.

CEDPO
CONFEDERATION OF EUROPEAN
DATA PROTECTION ORGANISATIONS

Table of Contents

1. Does the GDPR regulate artificial intelligence and machine learning?

Yes, the GDPR does regulate AI and machine learning. The GDPR regulates all forms of technology that process personal data. As a horizontal, risk-based, omnibus regulation, which governs on the general, rather than the specific level, the GDPR espouses broad principles that apply regardless of the particular context in which personal data is processed. This is in contrast to vertical, rules-based regulation that specifically legislates for defined technologies or sectors.

The effect of this is that, with respect to technology, the GDPR is explicitly technology-neutral. The words 'AI' or 'machine learning' do not appear anywhere in the text of the GDPR, but neither are there any references to blockchain, Internet of Things, non-fungible token (NFTs), virtual reality, nor any other emerging technologies. The absence of such references is intentional and not accidental. The logic of the legislators was that if specific technologies were mentioned, this could allow as-yet unknown, future technologies to evade the scope of the regulation. As Recital 15 states: 'In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used.'

The above principle of the GDPR's technological neutrality was also examined and upheld by the Court of Justice of the European Union in Case C-25/17 *Tietosuojavaltuutettu and Jehovan todistajat — uskonnollinen yhdyskunta*. The Court's Grand Chamber noted that with respect to 'the protection of individuals ... the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention.'[1]

The GDPR, is thus future-proofed by providing high-level principles that can be adapted for any emerging technology, or, indeed, for any unforeseen data processing purposes. For example, the response to the Covid-19 pandemic in 2020, demonstrated how the GDPR's existing general principles could be successfully applied to an unexpected emergency that led to the rapid creation of new, potentially privacy-invasive technologies, such as Covid-19 track-and-trace applications.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CJ0025

Regardless, then, of the mode, appearance, technique, context or use, if any AI or machine learning technology processes personal data, the GDPR applies. For instance, the current evolution of powerful large-language models, such as ChatGPT, was not specifically anticipated or envisioned when the GDPR became law in 2018, however, it is clear that this and other such developments are subject to the scope of the GDPR, and must conform to its principles.

2. Does automated processing always involve AI or machine learning?

No, there are many cases where automated processing does not involve AI or machine learning. Recital (15) EU GDPR confirms that automated processing refers to processing via automated means, in contrast to processing which is conducted manually. Data processing operations will frequently be 'automated' without any AI or machine learning component being involved. For instance, customer relationship management (CRM) tools will involve automated personal data processing (through computer systems), without necessarily involving AI or machine learning.

The same reasoning applies to the two core concepts outlined in the European Data Protection Board's (EDPB) Guidance on Automated individual decision-making and Profiling for the purposes of regulation 2016/679:[2] Although AI and machine learning can be expected to become increasingly important, both automated decision-making and profiling have been and can still be applied without using AI.

Profiling is defined in Art. 4 of the EU GDPR as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.' However, as stated, profiling does not always involve AI or machine learning and this is borne out by many use cases.

For example, e-commerce businesses have been using profiling to understand the interests and preferences of individuals, and then suggest relevant products, long before AI or machine learning became more prevalent.

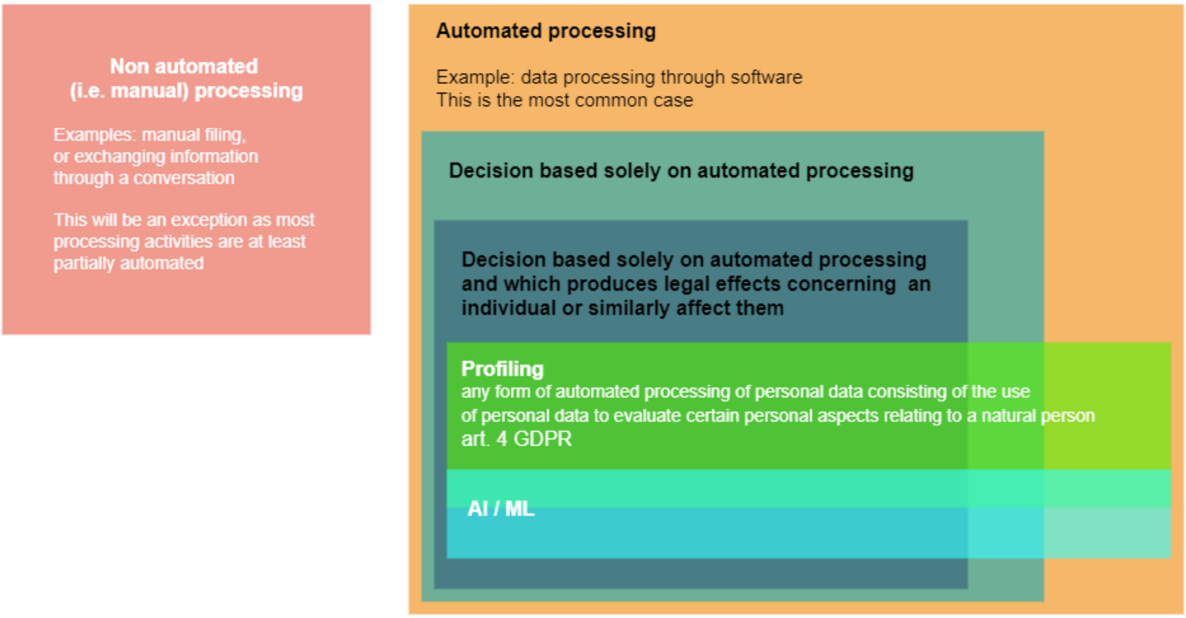
Decision-making based 'solely on automated processing and which produces legal effects, or similarly affects individuals', is covered in the EU GDPR, in particular, in Recital (71) and Article 22. Recital (71) provides two illustrations: the 'automatic refusal of an online credit application'

[2] https://ec.europa.eu/newsroom/article29/items/612053/en

or the use of ‘e-recruiting practices without any human intervention’. Clearly, such decisions will not always involve AI or machine learning.

For example, and as detailed in the above-referred EDPB guidance on Automated Individual Decision-making and Profiling, an automatic refusal of an online credit application can be implemented with an algorithm that assesses an application against a set of criteria, such as information provided on the application form, or information about previous account conduct including payment arrears. These can be implemented without AI or machine learning.

The following diagram shows how the concepts of automated processing, AI and machine learning converge and diverge:


Non automated
(i.e. manual) processing
Examples: manual filing,
or exchanging information
through a conversation
This will be an exception as most
processing activities are at least
partially automated
Automated processing
Example: data processing through software
This is the most common case
Decision based solely on automated processing
Decision based solely on automated processing
and which produces legal effects concerning an
individual or similarly affect them
Profiling
any form of automated processing of personal data consisting of the use
of personal data to evaluate certain personal aspects relating to a natural person
art. 4 GDPR
AI / ML

3. Do AI and machine learning always involve the processing of personal data?

No, AI and machine learning systems do not always involve the processing of personal data. They can be used for various purposes, which may have no connection with personal data, such as weather prediction, where the data input consists of atmospheric measurements from sensors, or precision farming for optimizing the use of pesticides and nutrients. Therefore, there are numerous instances where AI and machine learning systems process non-personal data.

However, the datasets processed by AI systems should be examined in more detail, even when these systems do not a priori involve personal data. It is important to note that non-personal data can be of two types: data that originally did not relate to an identified or identifiable natural person and data that was originally personal but was subsequently anonymised. Anonymised data cannot be attributed to a specific person, even using additional data. However, if non-personal data can be linked to a person in any way, making him or her directly or indirectly identifiable, this data must be considered as personal data. Several examples of re-identification of supposedly anonymous datasets have shown that particular care is needed when anonymising datasets.

The case of mixed datasets should also be considered, as these datasets consist of a combination of personal and non-personal data. The boundary between personal and non-personal data is therefore sometimes blurred and within a mixed dataset, personal and non-personal data may even be inextricably linked. This type of dataset is particularly common with new technological developments such as the Internet of Things, but also AI and machine learning systems. In this case the GDPR will apply.

Once the question of whether the data contained in the datasets are personal or not is considered, another issue needs to be addressed.

It should be noted that the implementation of an AI system takes place (generally speaking) in two phases, the training phase and the production phase. In the training phase, the AI system learns from a set of data, creating a model capable of making predictions or decisions. In the production phase, the trained model is applied to new data to generate results, such as predictions, recommendations or decisions. These two steps do not serve the same objective and should therefore be separated.

It is thus possible for an AI system to involve the processing of personal data in both its training and production phases, but also only in one of the two phases. In this respect, it is necessary to study all the stages of the AI system implementation process.

Furthermore, as we have already mentioned with the deduction of personal data from non-personal data, it is important to emphasise that even if AI systems are not explicitly fed personal data during these stages, they may still deduce personal information from non-personal data. Both input data and output data can involve personal information and one does not imply the other.

Considering all these aspects, we can say that AI and machine learning systems do not always process personal data, but it is essential to ensure that the data being used and generated are genuinely non-personal, where that is the desired goal.

One final qualification should be noted. Although the core processing activities of an AI tool may not concern personal data, it is still possible that it might process personal data linked to the actual human user of it. This can be linked to the account needed for using the AI system as well as "usage data" that can directly or indirectly identify an actual person. Some personal data might even be inferred from such a use case, from the final user or a third person, especially with generative AI.

4. Do any articles and recitals of the GDPR specifically apply to AI and machine learning?

The GDPR applies to all processing of personal data; therefore, in its most basic sense, whenever an AI or machine learning system is engaged in the processing of personal data, then GDPR applies to those circumstances. It is important to note that these obligations apply now. A DPO should not wait for formal regulation of AI by the European Commission through the proposed AI Act in order to ensure that an organisation's use of AI complies with its data protection obligations under the GDPR. The GDPR, of course, is technologically agnostic, and does not contain specific references to AI or machine learning-based processing per se.

Notwithstanding this, there are nuances that need to be considered. In the first instance, not all AI or machine learning systems involve the processing of personal data, and so GDPR would not apply; further, Article 2(2) of the GDPR provides for various exceptions, and the use of an AI or machine learning system in these circumstances would also be excluded under these exceptions (whether processing personal data or not).

There are a number of ways that AI and machine learning systems can come into contact with personal data, including:

- It may be part of the data set used to "train" the system
- It may be searched, from the internet, for example, in pursuit of a query (note that so far as GDPR is concerned, it does not matter if the data is otherwise public)
- It may be provided by the end user as part of a query or other input
- It may be generated, through inference, or association via pattern matching etc.
- It may, given limitations inherent in the generative model, simply make stuff up i.e. generate plausible content or "hallucinate".

Whenever an AI or machine learning system is processing personal data (regardless of how such data came to be in its possession) there are a number of articles in the GDPR that have direct application. These include:

- Article 5 (principles); the use of the AI or machine learning system, when involving personal data, must adhere to all the principles. As with any personal data processing system, a risk assessment should be carried out; particular concerns may exist around, for example, transparency, minimisation, and accuracy (see note on "hallucination" above). (see also Rec.39).

- Articles 4, 6, 7 (lawfulness of processing, consent); insofar as AI and machine learning systems are "trained" on large datasets, there must be an appropriate legal basis for this. It is perhaps the case that in many circumstances the concept of "legitimate interest" would be relied upon, but not that this has to be clearly established (Rec. 47). Certain circumstances (e.g. processing of special categories) require consent (Art.7), while training of the system may have been carried out under the basis of scientific research purposes, this basis lapses once the use of the system passes into the commercial domain.

- Articles 22 (Automated Decision Making); this area is the focus of much attention given the potential uses for AI and machine learning systems. Art.22 provides a right for data subjects to object to such processing, but perhaps of more interest is the corresponding right under Art.14.2(g) to be provided with "meaningful information about the logic involved", something which is challenging given the nature of the systems concerned.

- Article 25 (Privacy by Design); Art 25 requires the controller to take into account the "state of the art" in order to meet the requirements of the regulation. Given both the complexity and the uncertainties that surround AI and machine learning systems, extra protections may be needed to secure data subject rights. Note that Rec. 78 specifically calls out the "processing of personal data in fulfilling a task" as an area to which this applies.

- Articles 35, 36 (Data Protection Impact Assessment); Much of the above leads to the importance of DPIAs in this area. Potentially, AI and machine learning systems may be more likely to require a DPIA than more traditional information processing systems. There is a convergence here with the AI Act where systems are "high risk" (though note the meaning of "high risk" is different in each case); in this case, Art 36.1 requires prior consultation with the supervisory authorities, requiring those authorities to have appropriate technical bandwidth in this area.

5. If the GDPR already regulates AI and machine learning, then why we do we need the AI Act as well?

While the EU GDPR and the EU Artificial Intelligence Act (AI Act) might, ostensibly, seem like similar pieces of legislation, in that they both envisage accountability, governance and oversight regimes, it is important to first recognise that, in the context of AI and machine learning alone, they serve distinct regulatory purposes. On the one hand, the GDPR, which is concerned primarily with the protection of personal data, is technologically agnostic, and makes no explicit reference to specific technological applications (including AI or machine learning). On the other hand, the AI Act represents a more direct, hands-on approach to AI regulation, and seeks to establish a comprehensive regulatory framework to promote the responsible development and use of AI and machine learning-based systems in the EU.

The GDPR recognises that certain processing operations impact the exercise of fundamental rights and freedoms, namely, the rights to privacy and data protection, insofar as these types of processing activities involve the use of EU citizens' personal data. Given that the GDPR essentially applies to all processing of personal data, therefore, in its most basic sense, whenever an AI or machine learning system is engaged in personal data processing, then the GDPR applies in those circumstances. At face value, this approach is relatively straightforward; yet, there are nuances to be considered. Firstly, not all AI or machine learning systems require the processing of personal data, and so in those circumstances, the GDPR will not apply. Further, Article 2(2) of the GDPR provides that the use of an AI or machine learning system in certain circumstances is also excluded (whether processing personal data or not).

Given that not all AI and machine learning applications will result in activity which amounts to personal data processing, the AI Act recognises that the use and deployment of AI and machine learning systems represents an area of broader ethical and societal concern that will often fall outside the scope of the GDPR. For example, certain practices using AI or machine learning-based techniques might result in the perpetuation of cultural biases or discriminatory practices, or pose real-time safety and security risks. The GDPR may simply be of little relevance or application in these circumstances. Thus, given its limitations in addressing areas of broader concern which fall outside the scope of privacy and data protection, the AI Act undertakes to develop a comprehensive and technologically bespoke framework that will invariably complement the GDPR in its efforts to promote responsible AI innovation in Europe, while respecting fundamental Union rights and values.

6. How do some of the core principles of data protection apply to AI and machine learning?

As already stated, whenever personal data is processed via AI/machine learning systems, the GDPR applies generally to that activity and, so, necessarily, all the core principles of data protection apply. However, certain core principles of the GDPR have particular suitability and applicability to AI/machine learning contexts. In these cases, there is a strong overlap between data protection and AI governance.

Firstly, the foundational principle of transparency, as enshrined by Article 12 of the GDPR, is significant for the governance of AI/machine learning systems. In many such systems, it will not always be evident to data subjects that their data is being processed, in the background, as it were, by means of these technologies, nor will it be clear how these systems operate. In this respect, DPOs should be aware of the transparency requirements of the GDPR and the AI Act, both of which require transparency in different respects.

The GDPR imposes a general requirement of transparency when automated processing is taking place. Article 12 states: 'The controller shall take appropriate measures to provide any information … relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child'. For example, if your organisation's proposed use of an AI system will require the use of personal data collected directly from individuals to train a model, you must first consider whether you have complied with the transparency obligation under the GDPR and let data subjects know how their data will be used in the lifecycle of your AI system.

The AI Act, however, adds to this general requirement by imposing a number of specific transparency requirements. In particular, Article 52 imposes obligations with respect to the creation of so-called deep fakes that are based on AI/machine learning technology. Article 52(1) says: 'Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use.'

A further principle where data protection and AI governance overlap is that of fairness. Article 5(1)(a) of the GDPR creates a wide-ranging obligation that personal data be 'processed … fairly'. In the context of personal data processing, fairness is an intentionally elastic principle, designed to capture the myriad ways in which a party might process personal data unfairly. However, in the context of AI/machine learning, fairness tends to have a more definite application. For example, if as a DPO, you are considering the fairness of an AI/machine learning application, you will be concerned about the potential for bias and/or discrimination in the algorithms used. This might be racial bias, where the training data itself is biased against one particular race, or gender bias, where one gender is disproportionately affected. These cases amount to unfair processing of personal data.

Lastly, the principle of explainability, an AI governance term which means the extent to which a decision made by an AI/machine learning algorithm can be explained in human-legible terms, also has its analogue in the GDPR. In AI governance terms, the explainability requirement, to the extent that it is achievable, requires responsible parties to outline the causal links between input data and final decisions. DPOs should be aware that Article 14(2)(g) clearly states this requirement in the context of personal data, noting that 'meaningful information about the logic involved' in automated processing must be made available to data subjects.

7. AI and machine learning! They are the same thing, right?

AI and machine learning are two closely related but distinct fields of computer science.

AI refers to the broader concept of creating machines that can perform tasks that would typically require human intelligence to complete. This can include a range of technologies, such as natural language processing, robotics, computer vision, and more. The goal of AI is to create systems that can perform tasks that would typically require human intelligence, such as recognizing images or understanding natural language, and being able to make decisions. The level of capability of any AI system depends on the level and complexity of the system. Creating an AI system involves the development of algorithms and systems that can reason, learn, and make decisions based on input data.

Machine learning, on the other hand, is a subset of AI that focuses on the development of algorithms that can learn and improve over time. Essentially, machine learning involves teaching machines to learn from data without being explicitly programmed. In essence, machine learning is the process of training a computer to recognize patterns and make predictions based on large amounts of data. This can include supervised learning, unsupervised learning and semi-supervised learning. Supervised learning involves training an algorithm with labelled data, which means that the correct output for a given input is provided. The algorithm learns to map inputs to outputs based on the labelled examples it has been given. Unsupervised learning, on the other hand, involves training an algorithm on unlabelled data, and the algorithm must find patterns and structure in the data on its own. Semi-supervised learning is a combination of supervised and unsupervised learning, where some labelled data is provided, but the algorithm also has to learn from unlabelled data.

In summary, AI is a broader concept that encompasses a range of technologies, while machine learning is a specific subset of AI that focuses on the development of algorithms that can learn and improve over time.

8. I am a DPO. Should I be concerned about the growth of AI and machine learning?

As a DPO, you should indeed be concerned about the growth of AI and machine learning, as these technologies can lead to automated decision making that can potentially have serious implications for the rights and freedoms of data subjects. For example, AI can be used to make automated decisions regarding the pre-screening of employment candidates. Understanding how the algorithms work allows you to identify potential data protection risks and implement appropriate protective measures, wherever necessary.

Regardless of the size of your organization, as a DPO, you are going to be affected by the integration of AI and machine learning into your organisation's IT systems. For instance the following applications already use or plan to use them in the future:

- Microsoft Office plan to have AI and machine learning as early as this year, 2023;
- Many HR, payroll, sales and/or coding systems already use AI and machine learning and those that do not have plans to incorporate these technologies in the near future;
- Chatbots that use corporate and customer's personal data to provide personalized answers are already in use in many organisations and will only increase in use in the future.

As a DPO, you and your team will have to conduct Data Protection Impact Assessments (DPIAs) for all new data processing activities. In doing so, it is essential to understand the implications and limitations of the AI system, especially regarding any biases that could potentially exist. The potential for AI to generate inaccurate results must also be considered.

Furthermore, as already outlined in previous questions, in the near future, organizations that develop their own AI high-risk systems will be regulated not only by the GDPR but also by the AI Act. Examples of such high-risk systems can be found in the following scenarios:

- education or vocational training,
- for recruitment, evaluation or task allocation of employees,
- credit scoring of individuals,
- determining the eligibility of individuals to avail of social services and benefits.

As a DPO working for an organization that is implementing AI systems, you should play a role in the AI risk management procedure. Because it is a requirement under the GDPR to implement data protection by design and by default, the DPO is tasked with identifying, reducing or mitigating the known and foreseeable risks through adequate design and development of any AI systems that process personal data.

9. I have heard about ChatGPT and Generative AI. As a DPO, should I be worried?

ChatGPT currently is the most widely used Generative AI (or Gen-AI) model in the world, boasting more than 100 million users after just two months of its launch. Gen-AI is a category of artificial intelligence that can create a wide variety of content or data, such as images, videos, audio, text, and 3D models. As with other forms of AI, Gen-AI is trained on large amounts of data (for example, harvested from Internet web sites). A typical use case is to provide some input data and a request or prompt, which then guides the Gen-AI technology to create a response. The response can also be any form of data.

A number of concerns have been raised by European Data Protection Supervisory Authorities about ChatGPT's processing of personal data. The Spanish Data Protection Agency (AEPD) said in a statement in early April 2023 that it had opened an investigation into OpenAI, the developers of ChatGPT, to investigate 'a possible breach of the regulations' governing data protection in Spain.

AEPD's decision to investigate ChatGPT comes after a similar decision at the end of March 2023 by the Italian Data Protection Supervisory Authority (Garante per la protezione dei dati personali) to temporarily block the chatbot in Italy over concerns about its use of personal data belonging to Italian citizens.

The Italian Data Protection Supervisory Authority said there was no legal basis to justify 'the mass collection and storage of personal data for the purpose of 'training' the algorithms underlying the operation of the platform'. The authority also argued that since there was no way to verify the age of users, the app 'exposes minors to absolutely unsuitable answers compared to their degree of development and awareness'.

The Italian Data Protection Authority then later withdrew their blockage of the ChatGPT application on condition that OpenAI adopts a series of measures to protect the rights and freedoms of Italian data subjects, including:

- The provision of adequate information on the rights granted to data subjects, both users and non-users of ChatGPT, as well as details on how data is processed by the application.

- Demonstrating the explicit consent of data subjects or identifying the legitimate interest of the data controller as the legal basis for data processing.
- Implementing a system for verifying the age of users.
- Setting up technical and organizational measures for the exercise of the data subjects' rights, including those of rectification, deletion or the right to object to the processing of their personal data.

Additionally, ChatGPT is already inaccessible in several countries outside of Europe, including China, Iran, North Korea, and Russia.

As a result of these swift reactions to this new technology, DPOs must be vigilant and play a role in monitoring and raising awareness of the risks that this technology poses, especially the unregulated and potentially reckless use of such technologies with regard to the protection of individuals' personal data. Data input by users into ChatGPT may include personal, sensitive, or biometric data, governed by the GDPR, while other forms of data may include confidential or intellectual property, which is governed by organisational policies and/or other legislation.

A major responsibility of the DPO in relation to this technology is, thus, the promotion of an informed approach to the design, development and use of these Gen-AI systems. A range of governance and technical controls are also possible to allow DPOs to guide the appropriate use of Gen-AI services within their organisation, including:

- Data Protection and Information Security policies may require additions and updates.
- DLP (Data Loss Prevention) and related tooling may be configured to block or limit sharing of data with Gen-AI services or internet domains.
- Awareness and training programs are also appropriate, as the proliferation of Gen-AI services and the channels to use them will outpace technical means of governance.
- DPOs with international scope should also be aware of the dynamic legal status of Gen-AI services within several countries, both within the EU and globally.

In addition to unwanted sharing of data, Gen-AI also increases the risk of sophisticated phishing to obtain confidential data as it enables automation of emails and other communication and documents that resemble those of the organisation or of individuals.

10. Okay, so what are the key conversations I should be having internally to prepare for the emergence of AI and machine learning?

Going forward, DPOs should reach out and work closely with other stakeholders across their organization, such as data scientists, IT professionals, and legal experts and senior managers, to form an AI champion network (similar to a data protection champion network). This champion network will ensure that the use of AI technologies and systems in the organisation is transparent, accountable, and fair and most importantly that the use of AI is compliant with the GDPR.

Here are some steps that DPOs and their champion network can take to prepare for the increase of AI systems in their organisation:

1. Understand the AI technology: DPOs should have a good understanding of the AI technology being used in their organization. This understanding is aided by working with the champion network to understand department specific AI technologies, including how they work, what data they collect and process in each department, and what types of decisions the AI systems are capable of making.
2. Specify and clearly document the purposes of the data processing linked to the AI System: this is particularly important in both the design and development phase of the new AI system to ensure the validation of key GDPR principles like data minimisation and privacy by design and by default and in the roll-out of the AI system to the end users, especially in AI systems that process special category data such as health data.
3. Conduct data protection impact assessments (DPIAs): conducting a DPIA is a process that helps individuals identify and minimise the data protection risks of a project. DPIAs must be conducted whenever a project's data processing is likely to result in a high risk to the rights and freedoms of data subjects, as per Article 35 of the GDPR. DPOs should work in collaboration with the champion network and the various organisational departments to complete DPIAs to assess the risks associated with AI systems in each section of the workplace and to identify any potential impacts on individuals' privacy and data protection rights. A key part of a DPIA for AI systems is to check for any bias in the algorithm that could lead to discrimination.
4. Review data processing agreements: DPOs should review any data processing agreements with third-party AI providers to ensure that they include appropriate safeguards for the processing of personal data by AI systems.
5. Implement appropriate security measures: DPOs should ensure that appropriate security measures are in place to protect personal data from unauthorized access, loss, or destruction when using AI systems.
6. Monitor and audit AI systems: DPOs should monitor and audit the AI systems on a regular basis to ensure that they are functioning as intended and that data protection risks are being managed effectively.