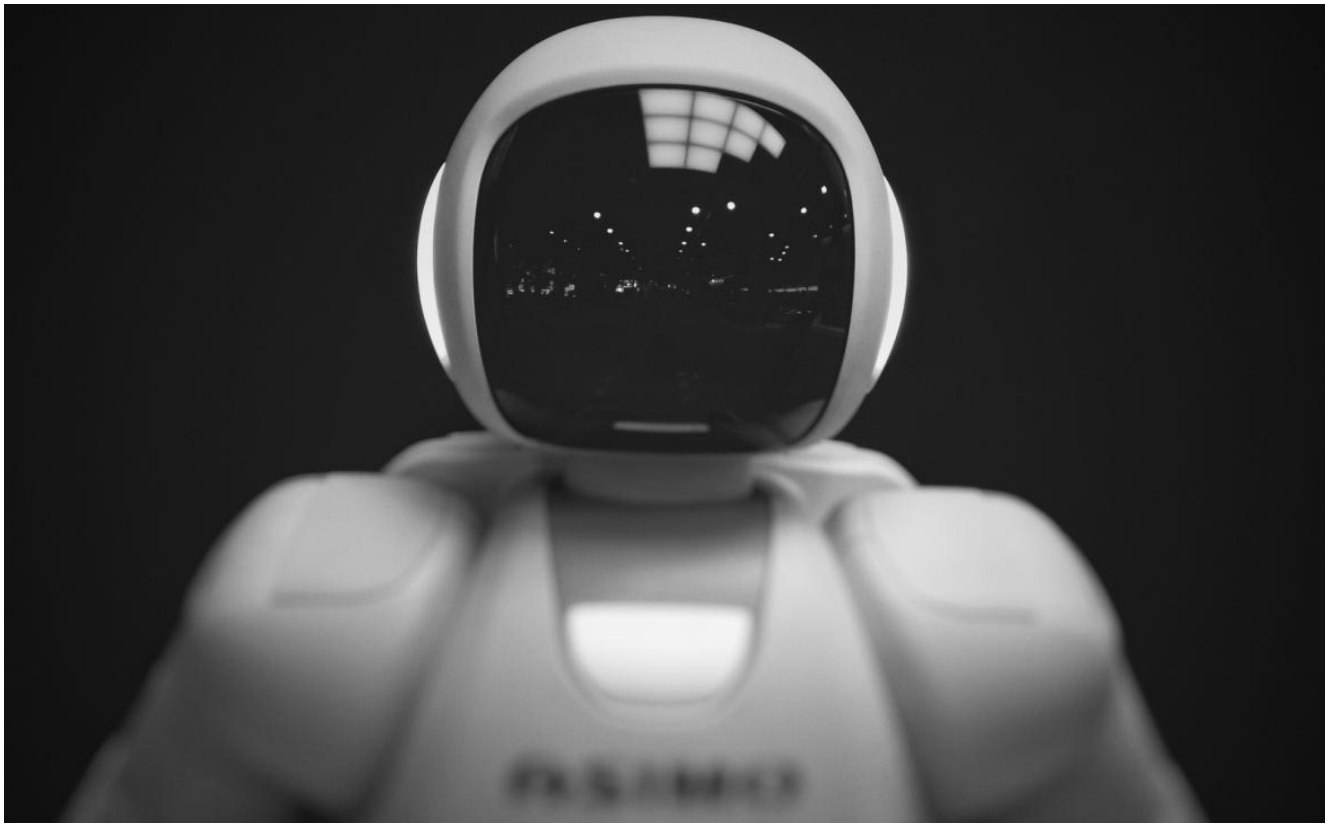
NJORD Estonia: Is it impossible to be GDPR-compliant in case of AI?

The use of AI-based technologies brings along various legal issues, such as liability questions regarding damages caused by using AI. When it comes to AI, there are data protection concerns as well. As explained in this article, it is difficult to comply with the core principles of data protection stipulated in Article 5 of the Regulation (EU) 2016/679 of the European Parliament and the Council (the "GDPR"). It is particularly problematic to achieve compliance with the principles of transparency, purpose limitation and data minimisation.



Principle of transparency

According to Article 5(1)(a) in the GDPR, personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. One of the principles stipulated in this clause is the principle of transparency. In practice, being transparent with data processing means that the controller must keep the data subject informed about how his or her personal data is being processed. According to Articles 13 and 14 in the GDPR, the controller must do this by giving specific information to the data subject. In practice, this information is usually given in a privacy notice or other document.

With regard to the obligation to inform data subjects about data processing, legal experts have already drawn attention to the so-called *privacy paradox*. The privacy paradox means that the less people understand how technology works and how it can be used to gather information about them, the more apprehensive they are likely to feel about it. In the case of AI, it is very difficult for people to understand how exactly the underlying mechanisms work.

Another aspect that has been highlighted by privacy experts is that traditional and unimaginative transparency mechanisms have their days outnumbered. Long and legalistic privacy notices, in particular, are unlikely to serve their purpose going forward. It has been suggested by legal scholars and by the European Data Protection Board that several other methods can be used to communicate information to a data subject effectively, aside from the traditional privacy policy. With regard to AI, some scholars have suggested that the next step is the adoption of very short "just-in-time" contextual notices. "Just-in-time" notices – like road signs – are there to help and can be developed in a way that blend into the right context, irrespective of whether they appear on a web page, a smartphone screen or a person's toaster display. Using "just-in-time" notices means that critical information about data processing is communicated to the data subject just before the data processing is about to take place.

Purpose limitation principle

Pursuant to Article 5(1)(b) of the GDPR, the essence of the purpose limitation principle is that a data controller must define the purposes of data processing. This must be done prior to the commencement of data processing. The aim of this is to keep data controllers from processing data for purposes that cannot be reasonably expected from the data subject. In the context of AI, we have the problem that AI-based technologies may process personal data for various purposes. Since AI is a mechanism that is able to learn, it may easily happen that the AI comes up with new purposes for data processing which may not be expected by the data subject. This issue is especially relevant when using AI in healthcare.

For example, let's imagine that AI is being used to invite persons to receive vaccines against a specific illness. The AI determines who should be invited to get a vaccine based on certain health and genetic data. Since AI is a human-like mechanism capable of learning, it can happen that the AI will be able to learn how to determine the onset of some other illnesses, based on the initially collected personal data and the personal data deduced from this. This constitutes a change in the purpose of data processing. In the case of AI, this kind of change in data processing purposes can happen frequently, while at the same time the data controller is, prior to the commencement of the processing for a new purpose, required to analyse whether the new data processing purpose is compatible with the initial one.

Data minimisation principle

According to Article 5(1)(c) of the GDPR, the data minimisation principle means that the personal data must be adequate, relevant and limited to what is necessary for the purposes for which the data is being processed. To comply with this principle, the data controller must ensure that it collects as little data as possible. However, this can be difficult to do when we want to utilise AI-based technologies as much as possible. For example, imagine that there is an AI-based service which is used to recommend new music to someone, as accurately as possible. In order to analyse someone's interests thoroughly to determine what would be a song to recommend, a vast amount of personal data may be collected by the AI. This can include conversations between people, recently visited places, recently read books and watched series, data about a person's mood and so on.

Conclusion

As we can see, compliance with the core principles of data protection is difficult to achieve in the case of AI. Regarding some principles, such as the principle of transparency, certain novel methods to achieve compliance have already been suggested by legal scholars, such as "just-in-time" privacy notices. Establishing compliance with other principles remains an issue yet to be solved.

TEA PARK (CIPP/E, CTO)
ATTORNEY AT LAW, SENIOR ASSOCIATE, CHIEF TECHNOLOGY OFFICER (CTO)

(+372) 66 76 440
TEA.KOOKMAA@NJORDLAW.EE

LIISI JÜRGEN
ATTORNEY AT LAW, PARTNER

(+372) 66 76 440
LIISI.JURGEN@NJORDLAW.EE