

DATA SOVEREIGNTY AND AI REGULATION: THE DEEPSEEK CASE AND THE CHALLENGES OF GDPR APPLICATION

Posted on 30 Aprile 2025 by [Roberta Romano](#)

1. At the end of January 2025, the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali, hereinafter also the "Garante") issued a [decision](#) imposing a definitive and immediate restriction on the activities of DeepSeek, a well-known Chinese artificial intelligence service that develops open-source large language models (LLMs). This measure was adopted pursuant to Article 58(2)(f) of the [General Data Protection Regulation](#) (EU 2016/679, hereinafter "GDPR") due to the opacity identified by the Italian authority in the data processing practices, which were deemed to endanger users' fundamental rights.

The decision was based on the following considerations. First, the privacy policy available on the website was found to be non-compliant with the requirements set out by the GDPR. Second, the authority observed that data were stored in the People's Republic of China, in violation of the rules on data security. Third and finally, the Data protection authority determined that no written designation of a data representative had been made, as required by Article 27 GDPR.

2. The measure in question stemmed in January from a brief exchange of correspondence between the companies managing DeepSeek (Hangzhou

DeepSeek Artificial Intelligence Co., Ltd. and Beijing DeepSeek Artificial Intelligence Co., Ltd.) and the Italian Data protection authority. The exchange involved a [request for information](#) from the latter regarding how Italian user's data were collected and stored by the service. Specifically, the *Garante* sought clarifications concerning the types of personal data collected, their sources, purposes of processing, legal basis, and whether such data were stored on servers located in China. Further inquiries addressed the information used to train the system and, in cases involving web scraping (i.e., the automated collection of data from websites), what information was provided to registered and non-registered users.

In response, the companies merely removed the app from Italian stores and stated that they had not entered the Italian market and had no intention of doing so. They further contended that the GDPR was not applicable to their data processing activities.

The day after DeepSeek's reply, the service was indeed rendered inaccessible in Italy, although the website remained online, albeit unavailable due to unspecified "malicious attacks". Nonetheless, those who had previously registered could still access it.

This was sufficient for the *Garante* to conclude that the Chinese companies' reply was inadequate, thus necessitating the swift interruption of the AI service on the Italian territory.

In particular, the data protection authority proceeded to analyse in detail the critical issues that emerged and the ways in which the applicable regulatory framework had been violated.

At a general level, the authority found a breach of Article 31 GDPR, as the companies' vague and non-cooperative reply contravened the obligation to engage with supervisory authorities in a spirit of cooperation. The *Garante* also reiterated that, under Article 3(2)(a) GDPR on territorial scope, this case involved the processing of personal data belonging to Italian citizens, therefore triggering GDPR applicability.

3. Turning to the core aspects of the decision, it examined the unlawfulness of the privacy policies on DeepSeek's website, identifying the absence of a privacy notice in Italian, the failure to indicate conditions of

lawfulness pursuant to Article 6 GDPR, and the lack of required information under Articles 12–14 GDPR. These omissions had significant consequences for the exercise of data subject rights as set forth in Chapter III of the GDPR. Indeed, the omission of lawful conditions under Article 6 of the GDPR, preventing the correct identification of exercisable rights, hinders effective control over personal data by the data subject. Moreover, the privacy policy should be clear and understandable: only in this way users can provide valid consent for the processing of their personal data. This implies, first and foremost, that such policies are also available in the language of the country where the service is provided (in this case, in Italian), and not limited to a generic announcement regarding data processing, instead of a precise and detailed list of lawful conditions for each ongoing processing activity, as required by Articles 12, 13, and 14 of the Regulation.

Another issue is the security of personal data processing. The storage of user data on servers located in the People's Republic of China was found to be in breach of Article 32 GDPR, which mandates the implementation of appropriate safeguards to protect individuals' rights and freedoms. Although the authority has not expressed a specific opinion on this matter, under Article 45 of the GDPR, transfers to countries outside the European economic area are permitted provided that the adequacy of the level of data protection is recognized through a decision of the European Commission. In the absence of such a decision, transfers are allowed only where adequate safeguards have been provided, as stipulated in Article 46 of the GDPR, which enumerates several possible measures (e.g., standard contractual clauses (paragraph c and d), codes of conduct (paragraph e), certification mechanisms (paragraph f)). In the present case, the People's Republic of China, not being among the countries recognized by the European Commission as providing an adequate level of protection, must provide suitable guarantees, such as those indicated under Article 46 of the GDPR.

Finally, a further violation was noted concerning Article 27 GDPR, due to the failure to designate in writing a representative in the Union for data processing activities. The provision in question requires that in the case of

data controllers established in countries outside the Union, the data controller or processor must appoint a representative of the European Union in writing. According to paragraph 4, Article 27, this representative is tasked with assisting or substituting the data controller or processor in dialogue with supervisory authorities and data subjects regarding ongoing processing activities. Similarly, Article 58 of the GDPR stipulates that the supervisory authority may obtain from the representative all relevant information necessary for the performance of its functions. Article 30, paragraph 1 of the GDPR further requires that the representative be responsible for maintaining the records of processing activities, together with the data controller.

On these grounds, the restrictive measure under discussion was adopted. This decision sparked international debate regarding the risks associated with the introduction of foreign AI systems into the European market and prompted reflection on the cultural differences in the understanding of data protection across jurisdictions.

Indeed, the Chinese equivalent of the GDPR, the [Personal Information Protection Law](#) (PIPL), highlights regulatory divergences that give rise to restrictive measures such as the one under review. The PIPL, which entered into force in November 2021, reflects a conception of personal data protection that is subordinate to pervasive state control. While it does provide for a consent regime, such consent may be overridden to facilitate cooperation with the state. Cross-border data transfers are permitted only with State approval. The government retains powers of access and oversight over all data held by companies and the law provides for sanctions that include operational restrictions imposed by public authorities.

It is precisely the broad discretion granted to the Chinese government and administrative authorities in managing personal data and safeguarding national security interests that comes into tension with the requirements of Chapter V GDPR, which allows personal data transfers to third countries only if an essentially equivalent level of protection is guaranteed as within the EU legal order.

This case has exposed the challenges involved in regulating AI systems at

the international level, particularly in terms of fundamental principles such as transparency and the accuracy of information provided to users whose data are transferred to countries with different, and often reduced, regulatory standards compared to the EU framework.

4. Italy has once again (as in [OpenAI case](#), commented also [here](#) in Diritti Comparati) acted as a forerunner, anticipating precautionary measures that were later adopted by other countries following the issuance of the restrictive measure.

In France, the national data protection authority (CNIL) announced its intention to question DeepSeek to better understand how the Chinese startup's AI system works and the potential privacy risks for users. In South Korea, similar statements were followed by a temporary [ban](#) on the service.

In Japan, following a government statement, the AI system was subjected to significant [restrictions](#)), as was the case in [Australia](#) and Taiwan.

Finally, in the United States, NASA blocked DeepSeek from its systems and employee devices after the U.S. Navy warned of "potential security and ethical concerns related to the model's origin and use".

In all these claims, the blocking of the program was justified by concerns over security risks posed by the Chinese application and the lack of clarity on how user data were processed, used, and stored by DeepSeek.

This short analysis aims to highlight the pivotal role played by the Italian case in fostering a broader debate on the entry of non-European AI systems into the EU context and on EU digital sovereignty.

It also invites reflection on the actual capacity of the GDPR to meet the challenges posed by global actors and, ultimately, to ensure the effective protection of users' fundamental rights at both the European and national levels.

Moreover, although the *Garante* has not expressed an opinion on the matter, it is worth questioning whether, and to what extent, the [AI Act](#) played a role in the case at hand.

The decision was indeed issued on 30 January 2025, but the provisions of the AI Act concerning transparency obligations for providers and deployers of certain AI systems (Title IV, Article 50, AI Act), as well as those

on general-purpose AI models (Title V, Articles 51 et seq.), will only become applicable as of 2 August 2026 and 2 August 2025, respectively. For this reason, the only legal grounds relied upon by the Authority were the GDPR and the [Italian Privacy Code](#) (Law Decree n. 196/2003). Nevertheless, it is reasonable to assume that, had the incident occurred during the full applicability of the AI Act, the *Garante*'s decision would have identified additional safeguards to be implemented for the protection of users, particularly from the perspective of transparency.

This post has been written within the remit of the research project 'SoBigData RI PPP - Preparatory Phase Project'. SoBigData has received funding from European Union - NextGenerationEU - National Recovery and Resilience Plan (Piano Nazionale di Ripresa e Resilienza, PNRR) under European Union's Horizon Europe research and innovation program (Grant Agreement No 101079043).