NEWSALERT

DATA PROTECTION & CYBERSECURITY

AI and privacy: the Italian Data Protection Authority's decision about the "Replika" chatbot

Introduction

In decision no. 232 of 10 April 2025 (the "**Decision**") the Italian Data Protection Authority ("**Authority**") imposed sanctions on the US company responsible for the AI-based chatbot "Replika" for violating Regulation (EU) 2016/679 ("**GDPR**"), which regulates personal data protection matters within the EU.

Developed and operated by Luka Inc., Replika features both a written and voice interface, allowing users to generate a virtual companion that can take on the role of a confidant, therapist, romantic partner, or mentor. According to the Authority, the company failed to meet various GDPR requirements, in particular those concerning minors' protection, user transparency, and the adequacy of its legal bases for data processing.

Consequently, the Authority: **(1)** ordered the company to comply with the provisions of the GDPR, particularly with respect to the age verification system, remedying the identified gaps and notifying the Authority of the initiatives taken to this end; and **(2)** imposed an administrative fine of 5,000,000 EUR.

I Key elements of the Decision

(1) Territorial scope of the GDPR. The Authority addressed the issue of territorial jurisdiction, specifically whether the GDPR applies to companies based outside the EU. It clarified that, in the absence of an effective EU establishment by the data controller (Luka Inc.), the "one-stop-shop" mechanism under art. 56 GDPR does not apply. Therefore, the competence to assess compliance with the GDPR and to exercise related powers lies with the Supervisory Authority of each Member State in which the company offers services or monitors the conduct of data subjects in the EU, pursuant to art. 3(2) GDPR (the so-called "targeting criterion"). The Authority noted that proof of services offered to Italian users was found based on the company's own statements, specifically its communication that it had *"promptly complied with the request for temporary*

restriction of processing for users established in the Italian territory, promptly inhibiting access to both the app and the website of the service from Italy". This statement, was considered sufficient proof that the service was offered to individuals in the EU.

(2) Transparency and language of the information provided to users/data subjects. The Authority found a formal non-compliance with the GDPR regarding the information documentation provided to Replika users, which also contained misleading and/or unclear information (*e.g.*, it did not clarify whether the service was offered exclusively to adults), thus constituting a violation of the information obligations under the GDPR. In addition, given the systematic nature and severity of the violations, the Authority deemed non-compliance with the general principle of transparency to be an additional and distinct violation. The Authority also reiterated that information must be provided in the language of the country in which the service is offered (in this case, it had been provided in English and not in Italian).

The general principle of transparency and fairness[1] expressed by the GDPR is concretely applied in the information documentation (privacy policy) that must be provided to data subjects/users of the service in accordance with Articles 12, 13 and 14 of the GDPR. These information obligations concern, *inter alia*, the purposes of the processing and the legal basis underlying each processing operation, as well as the period of retention of personal data and the presence of any transfers of personal data outside the European Economic Area. However, as the Authority noted, it is necessary to distinguish the compliance obligations deriving from the principle of transparency from the principle itself, which cannot be limited to specific requirements and can constitute an autonomous and further violation.

(3) Each legal basis shall be linked to a specific processing operation. The Authority considered that the legal bases outlined by the company were not linked or attributable to specific processing operations (so-called granularity), making it impossible to identify and evaluate the suitability of those legal bases. As it is the obligation of the data controller to demonstrate compliance with the GDPR, a general and implicit reference to the applicable legal bases in the privacy policy (*i.e.*, without clearly indicating which legal basis applies to each purpose) was deemed insufficient to demonstrate compliance with the legislation.

(4) The legal bases for interactions with the chatbot and the training of the AI model. In the Authority's view, the company should have specified in the privacy policy at least: **(i)** the legal basis of the processing for purposes strictly related to the use of the service ("Chatbot Interaction") and **(ii)** the additional legal basis for processing data for the purpose of developing the AI model underlying the chatbot. The Authority clarified that it will conduct an independent investigation into the identification of the suitable legal bases underlying the life cycle of the Replika chatbot system, specifically in relation to the fulfilment of contractual obligations with users and the legitimate interests of the data controller. The identification of a suitable legal basis, in relation to each purpose of the processing, is an obligation of the data controller in accordance with the principle of accountability.

(5) Obligation to implement age gate systems. The Authority found that the company had failed to implement suitable systems to verify the age of Replika users as early as 2 February 2023. The absence of a common European standard in this regard was not

[1] Art. 5, par.1, (a) GDPR.

considered a possible cause of justification for non-compliance. The Authority clarified that a suitable age gate system:

(i) should not be circumvented by the minors (*e.g.*, by changing the date of birth in the profile settings section or by using "incognito" mode);

(ii) should be able to block the user if obvious information about their age suggests they are underage (*e.g.*, by evaluating statements made to the chatbot); and

(iii) should provide a "cooling-off period" to prevent minors from entering a different date of birth when denied access to services.

(6) **Obligation to protect minors and vulnerable persons in compliance with the principles of privacy by design and by default**. According to the Authority, the company's failure to adopt suitable organizational measures and techniques to safeguard access to and use of the service by design, including in order to process relevant and necessary data in relation to the service offered, constituted an independent violation of the GDPR, also entailing a particularly high risk for minors and vulnerable data subjects.

The Authority highlighted the recent news cases relating to episodes of self-harm related to the use of chatbots by vulnerable categories of data subjects.

In this context, the performance of a data protection impact assessment pursuant to Article 35 of the GDPR ("**DPIA**") as well as data protection processes by design and by default is particularly important. Notably, as the DPIA carried out by the company did not have a specific date, it was not considered suitable by the Authority for proving the temporal relevance of certain circumstances contained therein (*i.e.*, that the conditions of lawfulness referred to in Article 6 of the GDPR had been identified prior to the Authority's first intervention).

II Conclusions and takeaways

The Decision is a significant development in the protection of personal data in relation to emerging technologies, such as chatbots based on generative AI systems. The Replika case, in particular, highlights the need for an increased level of accountability on the part of providers of related services when it comes to human-machine interaction, especially with potentially vulnerable subjects such as minors.

The territorial scope of the GDPR is one of the most sensitive matters and a frequently raised issue in proceedings involving non-EU companies. It is indeed a primary defensive argument, often used to limit exposure to EU authorities or direct proceedings towards a more favorable lead authority. However, as the Replika case shows, EU authorities require concrete, documented evidence of an EU establishment for the purpose of the applicability of the one-stop-shop mechanism. A robust and well-documented strategy on this issue is therefore crucial to avoid direct exposure to multiple national authorities and the risk of multiple sanctions and complex litigation management. For international companies offering digital services in the EU, it is essential to address the issue carefully and accurately assess their organizational structure and supporting documentation to prevent it from becoming a point of vulnerability.

In addition, the Authority's reminder to identify suitable legal bases for each processing operation ("principle of granularity"), provide transparent information in a user-friendly

language, adopt a privacy-by-design approach, and implement effective age verification tools applies to all economic operators, including those in different sectors and those active outside the EU but providing services to individuals located in Italy.

Regarding age gate systems, the Decision contains useful clarifications about the obligations of data controllers and the technical measures they can adopt. However, many issues remain unresolved. Therefore, it is crucial for economic operators to assess the suitability of the age gate systems implemented for the service offered on a case-by-case basis.

In this context, it is also relevant to recall the guidance set out in EDPB Statement 1/2025 on age assurance, which emphasizes the importance of robust governance to ensure the full accountability of the controller. The Statement emphasizes the necessity for organizations to establish internal processes and policies that enable them to monitor, review, and document the operation of age verification systems throughout their lifecycle. This includes defining clear roles and responsibilities, preparing audit mechanisms, and ensuring the effective implementation of risk management procedures. Chiomenti's professionals can support you in implementing these processes, offering assessment and strategic consulting services to ensure that the solutions adopted always comply with best practices and regulatory developments.

Finally, it should be noted that, should the Authority actually decide to initiate an independent investigation into the correct identification of the legal bases underlying the use of the chatbot and the post-training of the underlying generative AI model, this investigation could result in concrete indications for the widest audience of parties interested in the adoption or offer of similar technologies and services.

Contacts

Pierluigi Perri
Of Counsel – Chiomenti
Data Protection & Cybersecurity
T. +39 02 721571
pierluigi.perri@chiomenti.net

Marilena Hyeraci
Of Counsel – Chiomenti
Data Protection & Cybersecurity
T. +39 02721571
marilena.hyeraci@chiomenti.net

Matteo Leffi
Senior Associate – Chiomenti
Data Protection & Cybersecurity
T. +39 02 721571
matteo.leffi@chiomenti.net

Tommaso Bratina
Junior Associate – Chiomenti
Data Protection & Cybersecurity
T. +39 02721571
tommaso.bratina@chiomenti.net