

(English version)

**Question for written answer E-000056/26
to the Commission
Nicolás González Casares (S&D), Laura Ballarín Cereza (S&D)
(9 January 2026)**

Subject: Data privacy and security risks posed by AI and browser extensions harvesting AI chat conversations

A recent cybersecurity investigation found that several widely used browser extensions that were advertised as privacy or security tools were secretly collecting users' AI chat conversations. According to Koi Security, this data collection could not be disabled without uninstalling the extension, it affected over 8 million users, and it involved transmitting complete AI prompts and responses, timestamps and session data to third-party servers for marketing analytics — despite the extensions being promoted with trust badges that may have misled users.

In the light of the above,

1. Does the Commission consider that the automatic collection and commercial sharing of users' private AI interactions — often involving highly sensitive personal, health, financial or proprietary information — without clear, informed and granular consent, constitutes a breach of EU data protection and AI governance frameworks?
2. What measures will the Commission take to ensure digital marketplaces effectively enforce platform policies and prevent the use of browser extensions that engage in covert data harvesting from being promoted with trust signals (e.g., 'featured' badges) that imply user safety?
3. In relation to AI governance and cybersecurity, does the Commission plan to propose specific regulatory guidance, additional safeguards or enforcement action to address the privacy risks associated with AI services and with browser extensions that intercept AI service communications?

Submitted: 9.1.2026

**Answer given by Mr McGrath on behalf of the European Commission
(17 March 2026)**

The processing of personal data requires a lawful ground under the General Data Protection Regulation (GDPR). ⁽¹⁾ Consent is only one of the six lawful grounds for processing. ⁽²⁾ It is the obligation of the controller to select the most appropriate ground. ⁽³⁾

If the conducted activity involves storing or accessing information stored in the users' terminal equipment such activity must also comply with the e-Privacy Directive which requires user's consent, subject to limited exceptions. ⁽⁴⁾ That consent must comply with the GDPR.

The enforcement of the rules of the GDPR and the e-Privacy Directive in individual cases, such as the case at hand, lies with the national supervisory authorities and courts.

The Cyber Resilience Act (CRA) ⁽⁵⁾, which starts to apply in full in December 2027, introduces mandatory cybersecurity requirements for manufacturers of products with digital elements, which may also cover browser extensions.

Accordingly, manufacturers must follow a security-by-design approach. Amongst others, the products must protect the integrity of stored, transmitted or otherwise processed data, personal or not.

The Artificial Intelligence Act (AI Act) ⁽⁶⁾ includes rules on high-risk AI systems which may apply depending on the intended use of the chatbot.

The rules provide for risk management and cybersecurity requirements appropriate to the risks. Providers must therefore implement security controls, which may include securing the interface of the AI system when communicating with the browser extension.

⁽¹⁾ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1-88.

⁽²⁾ Article 6(1) GDPR.

⁽³⁾ Article 5(2) GDPR.

⁽⁴⁾ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.

⁽⁵⁾ Regulation (EU) 2024/2847.

⁽⁶⁾ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

Requirements for high-risk AI systems should start to apply by August 2026, however, the Digital Omnibus on AI ⁽⁷⁾ proposes to postpone that deadline until standards and relevant tools are available to ensure a clear compliance pathway for providers.

⁽⁷⁾ Proposal for a regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI).