

Committee: European Parliament

Country: Spain

Delegate: Beren Başpınar

Political Group: European People's Party (EPP)

Spain acknowledges that data protection and data sharing stand at the core of the European Union's future. In the digital era, where cyber threats, disinformation, and international crime are on the rise, cooperation between Member States has become essential. However, this cooperation must not come at the expense of fundamental rights. As a representative of Spain and the European People's Party (EPP), I affirm our commitment to upholding the values of democracy, individual liberty, and the rule of law—principles that must shape every policy on data governance.

The General Data Protection Regulation (GDPR), implemented in 2018, has provided the EU with a globally recognized framework that respects individuals' rights while setting a standard for responsible data management (1). Spain has fully incorporated this regulation into its national law and continues to monitor and adapt its implementation through the Spanish Data Protection Agency (5). In parallel, Council Decision 2009/917/JHA, which facilitates the use of information technology for judicial and law enforcement cooperation, must be revisited to ensure that it aligns with modern technological realities and complies with GDPR principles (3). While data sharing is a critical tool in tackling cross-border crime, Spain believes that it must be conducted transparently, under democratic oversight, and with strict limitations on scope and duration.

Spain supports the development of a European Secure Data Sharing Framework (ESDSF) to ensure encrypted, transparent, and interoperable data flows between Member States. We propose that this system be overseen by the European Data Protection Board (4) with enhanced authority to monitor and enforce compliance with EU-wide standards. Furthermore, Spain urges investment in privacy-enhancing technologies such as differential privacy, blockchain-based ID verification, and AI-powered anomaly detection—tools that can reinforce both security and liberty. Public-private partnerships should be encouraged to develop secure cloud infrastructures for use in criminal investigations and border control, provided that these platforms remain subject to EU legal safeguards.

As an EPP delegate, I strongly believe in promoting innovation without compromising fundamental rights (6). We must foster a digital Europe where citizens trust institutions with their data because they know it will be protected. The path forward requires harmonized legislation, technological advancement, and above all, a renewed political commitment to the founding values of the European Union. Spain stands ready to cooperate with its fellow Member States to build a secure, transparent, and citizen-focused data ecosystem (2).

References

1. European Commission. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 – General Data Protection Regulation (GDPR). EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>
2. European Union. (2012). Charter of Fundamental Rights of the European Union. EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT>
3. Council of the European Union. (2009). Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs and police cooperation. EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009D0917>
4. European Data Protection Board. (2024). Annual report 2023. <https://edpb.europa.eu>
5. Agencia Española de Protección de Datos. (2023). Guía para la aplicación del Reglamento General de Protección de Datos (RGPD). <https://www.aepd.es>
6. European People's Party. (2022). Digital innovation and European security: Policy paper. <https://www.epp.eu/papers/>