

**Council of the EU (ECO)**

António Costa - President  
Unit Transparency (COMM) – Ref 07/c/01/25

**European Commission (COM)**

Michael McGrath – Commissioner  
TAXUD. D2; JUST-C1 and C3

**European Data Protection Board (EDPB)**

Ms Anu Talus - Chair

**European Ombudsman (EO)**

Teresa Anjinho – Ombudsman – Ref. 2193/2025/MIG

**European Parliament -PETI**

Dolors Montserrat – Vice-Chair –Ref. 1088/2016

**Mishcon de Reya**

Africa House

70 Kingsway

London WC2B 6AH

DX 37954 Kingsway

T: +44 20 3321 7000

www.mishcon.com

London | Cambridge | Oxford | Hong Kong | Singapore

28 September 2026

Dear Commissioner, Commission Services, President, Chair and Ombudsman

**Government hack situation is absolutely insane**

Over the past few months, we have been seeking to engage with EU institutions on the implications of a spat of cyber-attacks and cyber threats for EU systems of bulk collection of sensitive personal and financial data<sup>1</sup>.

Hacks include the theft of the entire database of an EEA Member State, the Hacking of the French Tax System, the French Interior Ministry, the French Ministry of Economy and Finance, a Lithuanian registry, the Berlin State Hack, the hacking of the Italian government's secure email system that enabled criminals to pose as government officials and trick Revolut to hand over the files of hundreds of customers to hackers.

Beyond the EU, the US Treasury confirmed that the IRS's IT systems remain inadequate, and the FBI confirmed that it is "aggressively investigating" a hack of its systems. This is directly relevant for FATCA, under which EU Member States automatically transfer the sensitive data of millions of EU citizens to the IRS on an annual basis without any indicia of wrongdoing.

To date, the EU has refused to engage with [EU FATCA Petitioners](#) and data protection/data security campaigners, notwithstanding very recent CJEU case law requiring safeguards (C-798/24).

On 11 September 2026, the European Council reiterated its refusal to grant access to internal documents that discuss internal data protection concerns around bulk systems of data processing introduced under EU law.

In the meantime, reports of institutional infightings have started to emerge in media reports, presumably with the help of whistleblowers, with Council legal services and EU Member States seemingly at loggerheads on how to make the situation legal (see [here](#) and [here](#)).

Once again, we ask the Council, the Commission, the EDPB and the European Ombudsman to address the existing concerns openly, release internal documents and start an active debate with EU Petitioners and data security campaigners to put an end to years of institutional obfuscation, deference, lack of transparency, lack of accountability - a situation described as "Kafkaesque" by MEPs and criticised by the European Parliament (Resolution P8\_TA(2018)0316).

**Filippo Nosedà**

Partner

<sup>1</sup> See our letters to ECO dated [5 August 2025](#) (central registers and ECB/FSB warnings), [6 August 2026](#) (META's acknowledgment of agenting AI hacks), [14 August 2026](#) (Attack against French Tax System), [28 August 2026](#) (more agenting AI-hacks), [7 September 2026](#) (Berlin State Hack), [24 September 2026](#) (Revolut hack and additional warnings about AI powered hacks); see also EO complaint dated [11 September 2026](#).