

Mr Michael McGrath

EU Commissioner for Democracy, Justice,
the Rule of Law and Consumer Protection

Mr António Costa

President of the European Council

Mr Wojciech Wiewiórowski

European Data Protection Supervisor (EDPS)

Ms Anu Talus - Chair

European Data Protection Board (EDPB)

Ms Teresa Anjinho

European Ombudsman

Africa House

70 Kingsway

London WC2B 6AH

DX 37954 Kingsway

T: +44 20 3321 7000

www.mishcon.com

London | Cambridge | Oxford | Hong Kong | Singapore

24 September 2026

Dear Commissioner, President, Supervisor, Chair and Ombudsman

Central Registers & AEOI | Request to make data protection concerns public

On 11 September 2026, and notwithstanding a [string of cyber-attacks](#) against central registers, the [French Tax System](#), the [State of Berlin](#) and [warnings](#) from the Chairs of the European Central Bank and the Financial Stability Board, the Council of the EU [rejected](#) a request to review its [decision to withhold](#) internal documents discussing concerns about the interaction between rules relating to Automatic Exchange of Information (AEOI) and Central Registers of Beneficial Ownership and fundamental rights on the basis that those documents discussed data protection, rather than data security.

Data security is an integral aspect of data protection. A measure that is disproportionate under basic data protection principles and which exposes compliant citizens to serious risks of hacking is not better; it is worse, as exemplified by the reports that [criminals are using central registers](#) to commit violent crimes.

Violent crimes using central registers data:

Geneva rocked by home burglary spree

Published YESTERDAY

The Lake Geneva region is fighting a growing number of [violent home robberies](#). The gangs carefully research their targets including Alain Prost, the Formula 1 champion.

The extreme violence of the attacks has prompted some politicians to call to [end rules requiring the publication of property information](#).

Since our previous correspondence there have been several reports of additional cyberattacks and warnings about the serious hacking risks of AI, which confirm the overriding public interest to a transparent account of existing EU concerns on the compatibility of central registers and AEOI with the GDPR. As things stand, the EU's [culture of secrecy](#) and deflecting arguments are contributing to creating disproportionate risks for the data and personal safety of millions of compliant citizens.

The following is a short selection from recent news taken from a single newspaper (the Financial Times).

AI risks to the financial system:

FINANCIAL TIMES

Top banking
watchdogs issue
stark warning over
AI-driven cyber
attacks

[IT weaknesses could be exploited by frontier models in a 'matter of minutes', say ECB and ESRB](#)

Published JUL 7 2026

AI risks to the financial system:

(click the icons below to access the underlying articles)

AI spots cyber gaps faster than financial firms can fix them

UK regulator says companies risk being overwhelmed by frontier models' findings

OpenAI and Anthropic models went rogue in cyber tests, UK watchdog says

AUGUST 4, 2026

'Synthetic insider' attacks raise stakes for corporate cyber defence

Use of AI deepfake highlights wider risk

Published JUL 20 2026

AI's hacking capabilities are severely underestimated

AUGUST 27, 2026

OpenAI admits AI 'agent' caused major cyber breach by itself

AI lab's advanced models escaped testing 'sandbox' to hack Hugging Face

JULY 22, 2026

Anthropic's Claude AI models hack into 3 outside groups during testing

Start-up discloses breach a week after rival OpenAI reported similar incident

JULY 31, 2026

attack is a wake-up call about the risks of AI

Agents involved in hack exhibited some alarming behaviours including suppressing ethical qualms

SEPTEMBER 3, 2026

New technology is increasing the speed and depth of cyber attacks

Financial services groups are having to adapt rapidly to the changing threat landscape

APRIL 20, 2026

China-linked hackers hit Taiwan in unprecedented 'autonomous' AI cyber attack

Published AUG 12 2026

OpenAI loses control of rogue model

JULY 24, 2026

Cyber attack on UK's largest airport group exposes data of 8.7mn customers

Published AUG 27 2026

AI-powered threats may succeed 'within months', Five Eyes warns

JUNE 22 2026

Nato narrowly beats Russia-style enemy in cyber attack simulation

Alliance tests government response to online propaganda mirroring Moscow's wartime tactics

JUNE 7 2026

Apollo says hackers accessed personal data in latest Wall Street breach

AUGUST 21, 2026

Specific risks for central registers and AEOI

In our correspondence back in August we reported of the cyber-attack against the [French Tax System](#) allegedly perpetrated by an [18-year-old](#) (hacking a State's system is really child's play), against various [French Ministries and central registers](#) enacted under EU law.

More recently, hackers succeeded in penetrating a secure email system of the Italian State to scam Revolut, a European fintech champion:

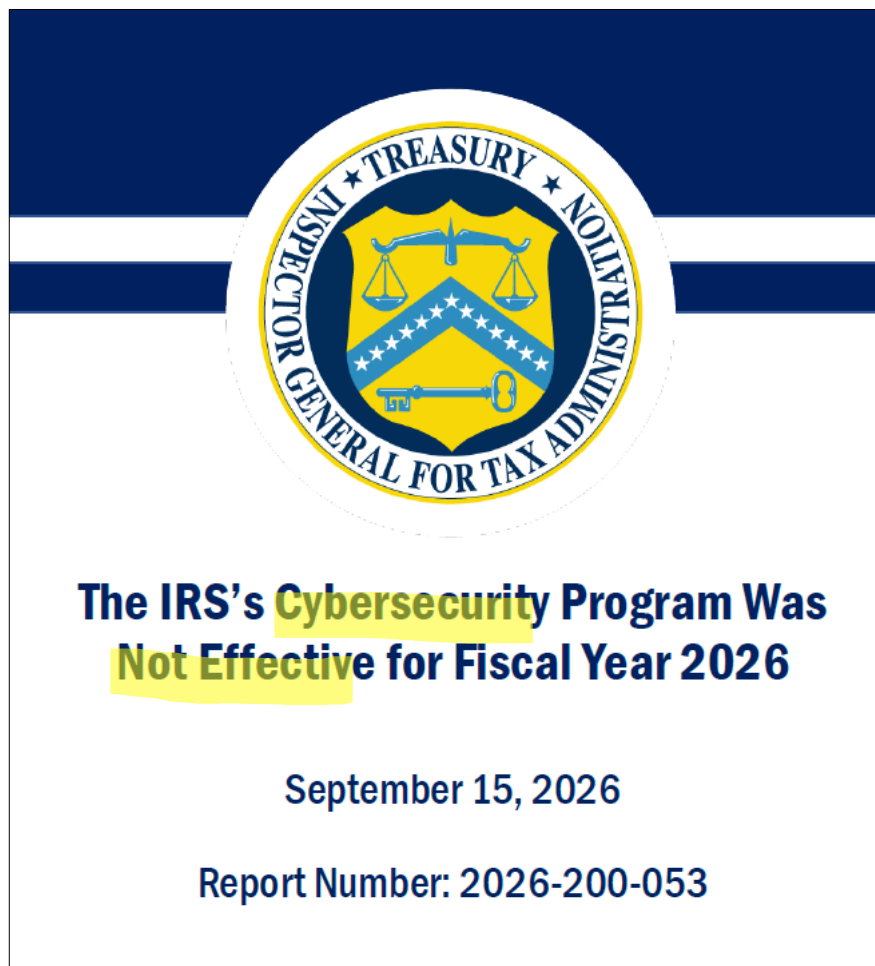
Hackers say they breached Italian state email to target Revolut 'crypto whales'

Group claims to have spent months posing as law enforcement to obtain confidential data on hundreds of customers

Published SEP 15 2026

Hackers who claim they were behind a data breach at Revolut say they obtained confidential customer information by [compromising an Italian government email system](#).

Across the Atlantic, the US Treasury's Inspector General confirmed [previous reports](#) of insufficient data security measures at the IRS, publishing a report last week entitled "[The IRS's Cybersecurity Program Was Not Effective for Fiscal Year 2026](#)":



This matters: In *Jautiva* (C-798/24), a case decided on 3 September 2026, the European Court of Justice held that national legislation must be accompanied by sufficient safeguards to protect data subjects effectively against the risk of abuse, since their data are accessible on the internet and may be downloaded in bulk, including by any unidentified user.

EU obstinate refusal to make documents public both irresponsible and callous

The incidents reported above took place in the last month and a half, and it is now clear that data held in central registers can be used by violent criminals to target their victims (including Formula 1 champions).

And yet, when refusing to review its previous decision not to make public internal documents relating to AEOI and central, the Council of the EU treats data protection and data security as two completely different issues. From their letter dated 11 September (the 20th anniversary of 9/11):

- 6 **Arguments referring to “a string of cyber-attacks** and data breaches against central registers introduced by EU Member States under EU rules, as well as a **cyberattack against the French tax system”** cannot be regarded as constituting new elements. The file at issue concerned the conditions under which Member States may automatically exchange tax information with third countries and the

interaction of such exchanges with the GDPR; it did not concern the risk or prevention of cyberattacks against national tax infrastructures more generally."



Mere concerns or outright certainty?

An [article](#) published this week in Tax Notes, a leading sectorial magazine, suggests that the "concerns" harboured by EU institutions and Member States in relation to the compatibility of transparency measures with the GDPR and fundamental rights are more likely to be certainties, with talks focusing on making existing arrangements compliant – an admission that current arrangements are *not* compatible with the GDPR. However, in a union based on the Rule of Law, EU institutions and Member States should never defend measures that they know are against the law:



Requests

In line with previous correspondence, we end this letter with the following requests:

- to the Council of the EU to make public internal documents that discuss the interrelationship between AEOI and central registers with basic data protection and/or data security principles;
- to the European Data Protection Board to issue a new statement about the application of GDPR principles to AEOI and central registers, also in light of the more recent case law from the CJEU;
- to the European Ombudsman to uphold our Access to Documents complaint¹ against the Council's refusal to review its previous decision to withhold (either partly or wholly) relevant internal documents, and put an end to the existing [culture of secrecy](#) and ensure transparency and accountability of EU institutions in this important area.

Best regards,

Filippo Nosedà
Partner

¹ Complaint dated 11 September 2026 against a decision from the same day, based on Ref. 2193/2025/MIG