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

Our Ref: FN/5999/60052.1

5 August 2026

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)

Dear Commissioner, President, Supervisor and EDPB Chair

EU bulk processing of information in the age of AI and cyber attacks

I am writing further to our previous correspondence to previous Commissioners, the EDPS and the EDPB, which is available online here and here. My testimonies before the European Parliament are available here and here; my *amicus briefs* to the CJEU in relation to beneficial ownership registers can be accessed here; my contribution to the EU's Discussion Paper on the CJEU judgment is available here; my presentation to the Council of Europe and the EU's data protection working party is available here; and my letter summarising the concerns raised by the European Banking Federation can be downloaded here.

This letter was prompted by the latest attack to a central register of beneficial ownership of an EEA Member State.

I have included a table of contents for ease of reference:

Table of Contents

***

Hacking of central registers of beneficial ownership created under EU/EEA rules

— Two days ago, the central register of beneficial ownership of an EEA State was hacked by unknown agents, causing the loss of the data of some 31,000 entities:

INDEPENDENT

Cyberattack hits Liechtenstein's register of people behind companies and foundations

— Previously, the president of the Luxembourg Law Society warned its members that agents were trying to purchase data contained in the Luxembourg RBE, which was at the centre of the recent CJEU case:

Barreau de Luxembourg

The Luxembourg Law Society has been informed that several members have been approached by an unauthorised entity seeking to retrieve data relating to the beneficial owners of local companies via your access to the Register of Beneficial Owners, in return for payment.

EU governments are unable or unwilling to protect registers from attack

Yesterday's cyber-attack came after a long series of similar incidents, including a cyber attack against the Lithuanian central register and several registers in France, all in the **last few months**:

LRT

Lithuanian police confirm mass registry data was stolen via Migration Department

News 2026.05.26 12:16

Lithuania's head of the Criminal Police Bureau Arūnas Maskoliūnas has confirmed that hundreds of thousands of records from national registries were stolen using accounts linked to the Migration Department.

Le Monde

Hackers pirate French Interior Ministry databases

Two highly sensitive databases were targeted: the judicial records system and the wanted persons file, which tracks individuals considered to pose a threat to national security. Interior Minister Laurent Nuñez said there has been no extraction of records at this stage.

December 17, 2025

Le Monde

Foreigners' data stolen in hack of French immigration agency

A hacker published several data samples online, including one containing the personal information of Israeli nationals living in France. The French Office for Immigration and Integration (OFII) confirmed the theft, but said the breach was linked to a subcontractor.

January 5, 2026

Le Monde

Hacker accessed data from 1.2 million bank accounts, French Economy Ministry says

The hacker used stolen credentials from an official, the ministry said. Owners of the affected bank accounts will receive notifications in the coming days.

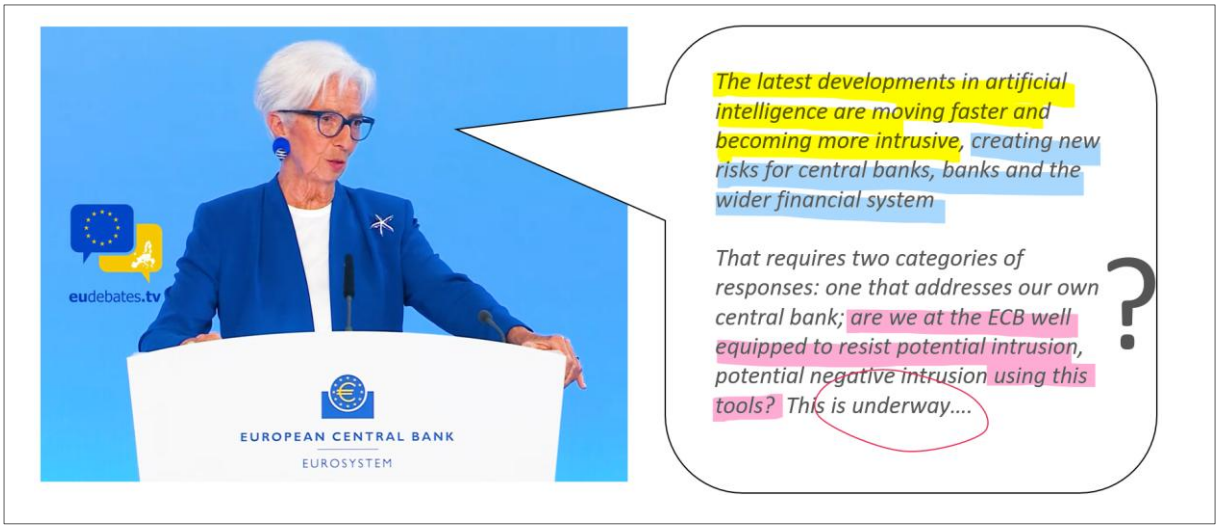
February 18, 2026

In the case of France, there was a deliberate attempt to defy the findings of the CJEU, which questioned the country's willingness to protect citizens' fundamental rights which are worth fighting for (as discussed in a letter appeared in the Financial Times).

AI is making things worse

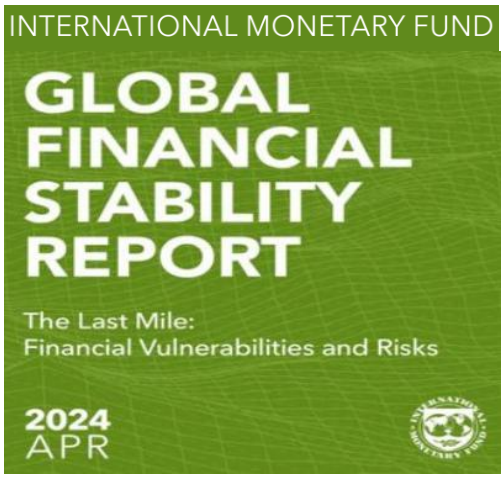
— This is another simple fact.

— The novel risks to data security posed by AI were addressed by the President of the European Central Bank in a recent interview on 12 June 2026, where Ms Lagarde acknowledged that the ECB's assessment of the capability of central banks and financial institutions to withstand attacks was still an open question and pretty much work in progress ("this is underway") – the same applies to central registers, which I am sure are subject to less stringent data security safeguards than, say, the internal database of the ECB:



— Two weeks later came the news that everyone was expecting: an AI programme started hacking into databases on its own:

— The implications for the global economy had already been identified by the International Monetary Fund in a report published in 2024 (and discussed in our previous correspondence).



Cyber incidents now pose an acute threat to macrofinancial stability because the sector is characterized by exposure to sensitive data, high levels of concentration, and strong interconnectedness—including with the real economy.

- Cyber-attacks are **not victimless**. The theft of personal and financial data that the CJEU rated sensitive in its judgment on BO registers can expose businesses and the families that control them to **phishing**, **identity theft** and **fraud**.

All despite concerns raised by EU experts and judicial setbacks

- In the past 15 years, the EU has developed policies that impose the **bulk processing** of sensitive personal and financial information of tens (and sometimes hundreds) of millions of compliant citizens, including central registers of beneficial ownership, central registers of bank accounts and automatic exchange of information.

- The aim of those policies has never been in question, notably the fight against money laundering and terrorist finance, which are **important aims**.

- However, it is the **necessity and proportionality** of the measures that have raised considerable concern from data protection experts, including the EDPS, the EDPB's predecessor, the Commissions own experts, and even the Commission itself (as summarised here and here).

- In the case of BO-registers, the Court of Justice of the EU (CJEU) waded in at the end of 2022 in a judgment that was discussed in a report published by the EU's AML/CFT Global Facility (available here), and we are now tackling the issues under the revamped framework that entered into effect on 10 July 2026, which effectively (a) re-introduces semi-public central registers of beneficial ownership; and (b) continues to require a central repository of all beneficial owners of EU/EEA structures, possibly as many as **33.5 million enterprises**, employing 164.2 million people (source: Eurostat).

- In the case of Automatic Exchange of Information, the compatibility of FATCA with the GDPR has been at the centre of a 96-page long ruling from the Belgian DPA and is currently before the CJEU (C-804/25).

Avoiding accountability as the current official currency

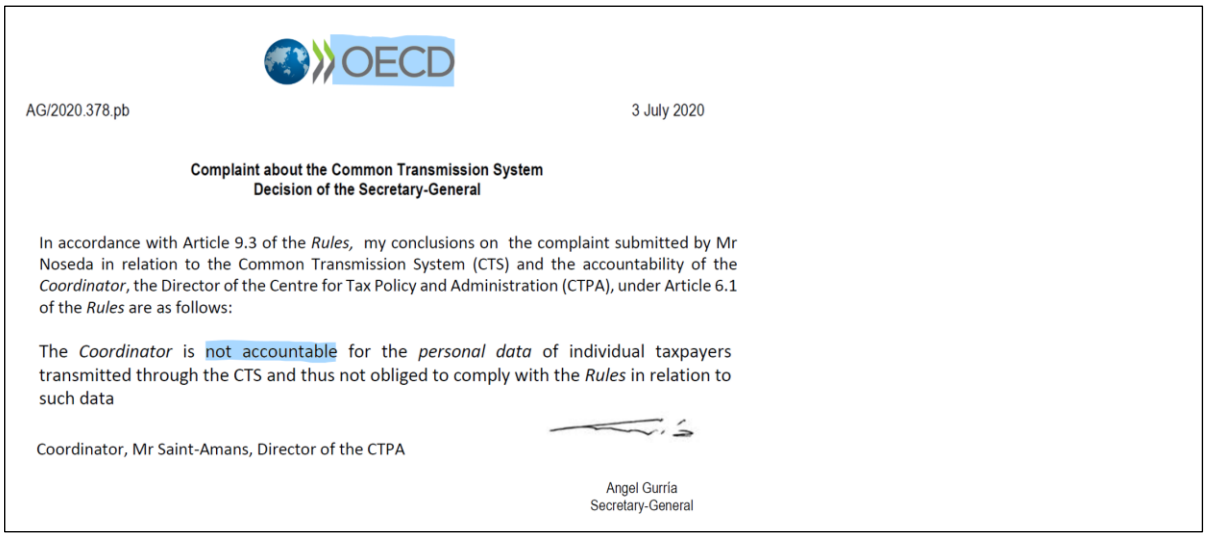
- The body of evidence shows that EU institutions and governments of EU/EEA Member States are **on notice** of the risks that rules they designed over a decade ago are causing citizens.

- Faced with the growing **inevitability** of a mass hacking of the sensitive personal and financial data of tens if not hundreds of millions of compliant EU citizens held on central registers of beneficial ownership, central registers of bank accounts and exchanged between tax authorities over the internet under systems of automatic exchange of information, tax authorities, EU institutions and even the OECD have started to peddle arguments aimed at **averting responsibility** and blaming someone else:

- EU institutions have been resolute in **refusing the disclosure of internal documents** evidencing existing concerns relating to the repercussions of systems of bulk processing of information for the safety and security of the personal data of compliant EU citizens. In the past, disclosure was forced by the EU Ombudsman (some of the documents are discussed here and here), who also made several findings of maladministration by EU institutions. What we have now are heavy redactions ("Guantanamo-style"), e.g. in relation to this steering note from the EU Presidency, **hindering transparency/accountability:**


Presidency steering note

— Separately, the OECD's Secretary General suggested in a letter to this firm following a formal complaint under the OECD Privacy Rules that his organisation owes is **not accountable** to ordinary citizens, despite the fact that its system of bulk processing of information now affects 171 million account holders:



OECD

AG/2020.378.pb 3 July 2020

Complaint about the Common Transmission System
Decision of the Secretary-General

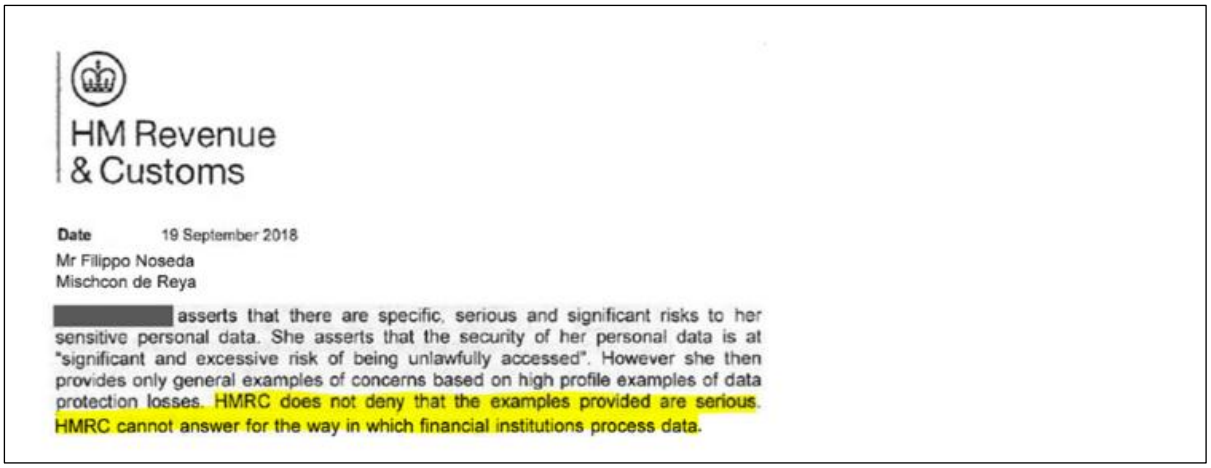
In accordance with Article 9.3 of the *Rules,* my conclusions on the complaint submitted by Mr Noseda in relation to the Common Transmission System (CTS) and the accountability of the *Coordinator*, the Director of the Centre for Tax Policy and Administration (CTPA), under Article 6.1 of the *Rules* are as follows:

The *Coordinator* is not accountable for the *personal data* of individual taxpayers transmitted through the CTS and thus not obliged to comply with the *Rules* in relation to such data

Coordinator, Mr Saint-Amans, Director of the CTPA

Angel Gurría
Secretary-General

— In the UK, the tax authorities blamed any attack on personal data on financial institutions, although the rules requiring the bulk processing of such data have been designed by the tax authorities themselves:



HM Revenue & Customs

Date 19 September 2018
Mr Filippo Noseda
Mischcon de Reya

[redacted] asserts that there are specific, serious and significant risks to her sensitive personal data. She asserts that the security of her personal data is at "significant and excessive risk of being unlawfully accessed". However she then provides only general examples of concerns based on high profile examples of data protection losses. HMRC does not deny that the examples provided are serious. HMRC cannot answer for the way in which financial institutions process data.

Urgent need for a reset and a new Social Contract on Data Protection

— While EU officials might not care much about Liechtenstein, the real question is: **who will be next**? Just France and/or Lithuania (discussed above)? Or all EU/EEA Member States?

— The GDPR was adopted in 2016 with the stated aim of **"giving citizens back control over their data"**. The main concern at the time (2016) was hacking and bulk processing of information by governments as revealed by Edward Snowden.

— In the decade that followed, there have been **countless instances of hacking affecting every level of society and EU/national governments**, including banks, judicial records, the Commission, Parliament, the European Court of Human Rights and even the US Treasury.

— In the EU, a proposal to water down the provisions of the GDPR (known as "Digital Omnibus") has sparked significant criticism and opposition, including from **Max Schrems**, the former Austrian law student who took on the Commission twice before the CJEU, winning both times.

— A few months ago, a former cabinet minister in the UK who was involved in the test case before the CJEU against the EU Data Retention Directive(C-203-15) penned this opinion in the Times pleading for a **new social contract** between governments and citizens when it comes to personal data:

THE TIMES

Government needs to get a grip on UK citizen's private data

While the value of data has soared, the protections afforded to the citizens who generate it have not kept pace

David Davis

Monday May 04 2026, 8.35pm, The Times

— The latest string of cyber-attacks against central registers in France, Lithuania and Liechtenstein requires a **reset of relations** between EU institutions and citizens.

Requests

Before it is too late, EU institutions should consider:

1. Advising EU Member States to **suspend** any bulk processing of personal data that may lead to irretrievable losses of sensitive personal and financial information of millions of EU citizens while investigations are underway;

2. **Carrying out an audit** of the data security arrangements deployed by EU institutions and governments of EU/EEA Member States to protect data held in central registers and/or exchanged over the internet as part of transparency measures designed in some cases over a decade ago. In the case of AEOI, the risks connected with the Common Transmission System (CTS) were highlighted in our correspondence to the OECD (accessible here, here and here);

3. In the case of the EDPS and the EDPB, **advising the Commission** and other EU institutions on the interaction between established data protection and data security principles on measures that entail the bulk processing of sensitive personal and financial data in the light of (a) the onslaught of cyber attacks affecting central registers; and (b) the novel risks posed by AI. To this end, the EDPS and the EDPB should be given full access to (a) the existing internal EU documents disclosed following the intervention of the EU Ombudsman (1398/2013/ANA); (b) the internal documents mentioned in our amicus briefs in the *Sovim* case (also here); as well as (c) the additional documents requested on 10 February 2025 (EU Ombudsman case reference 2193/2025/MIG);

4. Establishing a **group of independent experts** covering the fields of police enforcement/ AML/CFT, cyber-crime/cyber security and data protection to review cyber-incidents and discuss the risks posed by new technologies to the data of compliant citizens whose data is continually gobbled up by central registers. To this end, EU Member States should grant experts full access to data relating to existing incidents, whether they have been reported to local regulators (such as the CNIL in France) or not;

5. **Renewing their full commitment** to the principles laid down in the EU Charter of Fundamental Rights (in particular the provisions relating to privacy, data protection and necessity), the European Convention on Human Rights and the GDPR in the digital age;

6. **Confirming/extending the scope of GDPR sanctions** to EU Institutions/ EU Member States to ensure full protection (including through monetary sanctions) of affected citizens; and

7. **Engaging openly and transparently** with data protection campaigners, as well as EU Petitioners.

Best regards,

Filippo Noseda
Partner