



Opinion of the Advocate General at the Court Laila Medina in Case C-222/25 | Rahapesu Andmehbüroo

Press release No 145/26

Luxembourg, 8 October 2026

Advocate General Medina: The Law Enforcement Directive ¹ applies to the processing of personal data by the Financial Intelligence Units (FIUs) in the exercise of their mission to prevent, detect and combat money laundering and terrorist financing

Access of data subjects to the data processed by FIUs may be restricted, provided that the necessary safeguards are in place to prevent abuse

In December 2019 and January 2020, the Estonian Financial Intelligence Unit (RAB) rejected two requests by X for access to the information held by that unit about the exchange of information with financial institutions or foreign authorities concerning him. X challenged the decision before the national courts, and the Estonian Supreme Court ultimately ruled in his favour, holding that the GDPR ² applied to the processing of personal data by financial intelligence units.

Meanwhile, X submitted a new access to information from the RAB regarding any ongoing investigations into him. The RAB refused access again. Following a complaint lodged by X, the Estonian Data Protection Authority (AKI) ordered the RAB to reconsider its decision and grant X access to the requested information.

However, the RAB continued to refuse disclosure, maintaining in a series of decisions its obligation to preserve the confidentiality of the information contained in the RAB database in order to protect the Estonian financial system. X challenged these refusals before the national courts. At both first and second instance, the courts ordered the RAB to disclose the requested information.

The RAB appealed the judgment to the Estonian Supreme Court, which referred questions to the Court of Justice concerning the EU legal framework governing the processing of personal data by financial intelligence units. The questions essentially concern which EU data-protection rules apply, whether access to the information may be deferred until its destruction, whether a financial intelligence unit may refuse such access, and under what circumstances such a restriction is lawful.

In today's opinion, Advocate General Laila Medina delineates the legal framework applicable to Financial Intelligence Units (FIUs), such as the RAB. She emphasises that a proper balance must be struck between limiting access to personal data processed by the public authority in pursuing its legitimate aims, and safeguarding against any abuse, unlawful access or misuse of those data.

Firstly, the Advocate General recalls that the GDPR excludes the application of the general framework for data protection when two specific conditions are met: (i) the processing is performed by a public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties as well as any other body or entity designated under national law as possessing public authority or power for the same purposes and (ii) the processing operation is for the purposes of preventing, investigating, detecting, or prosecuting criminal offences, or executing criminal penalties.

When both criteria are met, the processing of the data **falls under the scope of the EU's specialised regime** namely

Directive 2016/680.

Financial Intelligence Units (FIUs), in the exercise of their mission to prevent, detect and combat money laundering and terrorist financing, fulfil both of these criteria and therefore qualify as competent authorities. Such qualification does not depend on the organisational structure of the FIU. In fact, EU legislation on combatting money laundering and terrorist financing³ requires FIUs to operate as independent and autonomous bodies with extensive powers to obtain information from law enforcement authorities and swiftly and decisively act against transactions that facilitate money laundering or terrorist financing. The missions, functions and powers of the FIUs demonstrate the importance of their role in crime detection and crime prevention in that field.⁴

Secondly, under EU law, a total prohibition on access to personal data held by FIUs may be compatible with their mission to safeguard strict confidentiality. However, any such restriction must comply with the principle of **proportionality**, which requires it to be limited in scope and duration to what is necessary to achieve the legitimate aim.

It must also **be anchored in legislation that provides clear and precise rules** governing its scope and application. This legislation must **provide the minimum safeguards necessary to prevent data abuse or unlawful access**, and enable the supervisory authority and the courts to exercise effective control over decisions regarding restrictions.

The conditions for restricting access rights in order to protect against misuse or unlawful access **may be set out** not only in a single legislative act, but also **in a coherent set of legislative and subordinate acts** that together define the limitations, provided that this set allows for a clear and precise understanding of the scope of the restriction and that it is foreseeable by the persons subject to it. However, in the present case, it does not seem that the applicable legal framework sets out clear conditions for restricting the right of access. It is for the national court to assess whether such restrictions comply with the standards set out in EU law.

Thirdly, to compensate for the absence of a direct right of access, **the rights of data subjects must be indirectly protected through the supervisory authority.** The authority must then be empowered to hold confidential discussions with FIUs to determine precisely which data are required for the data subject to obtain an effective judicial remedy.

Finally, EU law permits FIUs to refuse a data subject access request without providing reasons when disclosure would endanger the public interest. In such cases, however, **the FIU must inform the data subject of the possibility of exercising their rights indirectly** through the supervisory authority.

NOTE: The Advocate General's Opinion is not binding on the Court of Justice. It is the role of the Advocates General to propose to the Court, in complete independence, a legal solution to the cases for which they are responsible. The Judges of the Court are now beginning their deliberations in this case. Judgment will be given at a later date.

NOTE: A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice of the European Union about the interpretation of EU law or the validity of an EU act.

The General Court has jurisdiction to deal with requests for a preliminary ruling coming exclusively within the following areas (1) the common system of value added tax (VAT), (2) excise duties, (3) the Customs Code, (4) the tariff classification of goods under the Combined Nomenclature, (5) compensation and assistance to passengers in the event of denied boarding or delay or cancellation of transport services, or (6) the system for greenhouse gas emission allowance trading. The Court of Justice has jurisdiction to deal with all other requests for a preliminary ruling.

Neither the Court of Justice nor the General Court decides the national dispute itself. It is for the national court or tribunal to resolve the case in accordance with the ruling by the Court of Justice or by the General Court, which is similarly binding on other national courts or tribunals before which a similar issue is raised.

Unofficial document for media use, not binding on the Court of Justice. The presentation of the facts and the legal framework refers to the relevant period and is based on the case file.

The [full text](#) of the Opinion is published on the CURIA website on the day of delivery.

Press contact: Jacques René Zammit ☎ (+352) 4303 3355.

Images of the delivery of the Opinion are available on '[Curia Web TV](#)' and on '[European Broadcasting Service](#)' ☎ (+32) 2 2964106.

Stay Connected!



¹ [Directive \(EU\) 2016/680](#) 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (the Law Enforcement Directive).

² [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).

³ [Directive \(EU\) 2015/849](#) of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

⁴ The Advocate General considers that the Court of Justice's case law supports the conclusion that an entity acquires 'competent authority' status by virtue of its role in the data processing chain that underpins crime prevention, detection, and prosecution, precisely the function performed by FIUs (See Judgment of 30 April 2024 *La Quadrature du Net and Others* [C-470/21](#) – see also Press release [No 75/24](#), and Judgment of 21 June 2022 *Ligue des droits humains* [C-817/19](#) – See also Press release [No 105/22](#)).