Exchange of Information between Law Enforcement Authorities on New Footing

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

Thomas Wahl

Following the provisional agreement in November 2022 (→ eucrim 4/2022, 252-253), the Council and the European Parliament formally adopted the Directive on the exchange of information between the law enforcement authorities of Member States. The Directive (2023/977) was published in the Official Journal L 134 of 22 May 2023, p. 1.

It will repeal Framework Decision 2006/960/JHA on "simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union", known as the "Swedish Initiative".

The new Directive lays down the rules under which Member States' law enforcement authorities may exchange existing information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations.

AUTHOR

Thomas Wahl
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2023, Vol. 18(1) eucrim pp 36 – 39
ISSN: 1862-6947
https://eucrim.eu

CC BY ND

Scope and use of evidence

The Directive covers the exchange of information for the purpose of preventing, detecting or investigating criminal offences between the competent law enforcement authorities of different EU Member States.

It does not apply to exchanges of information for said purposes that are specifically regulated by other Union legal acts. It does also not impose any obligation on Member States to (a) obtain information by means of coercive measures; (b) store information for the sole purpose of providing it to the competent law enforcement authorities of other Member States; and (c) provide information to the competent law enforcement authorities of other Member States to be used as evidence in judicial proceedings.

Regarding the latter point, the Directive also clarifies that it does not establish any right to use the information provided in accordance with this Directive as evidence in judicial proceedings. Even though they are not required to do so, Member States providing information under the Directive, however, are allowed to consent, at the time of providing the information or thereafter, to the use of that information as evidence in judicial proceedings.

Main features

Key points of the Directive are Single Points of Contact established or designated by the Member States, to which requests for information must be submitted, the provision of information pursuant to such requests,

the working languages of the Single Points of Contact, mandatory time limits for providing requested information and the reasons for the refusal of such requests.

The exchange of information under the Directive is made subject to five general principles:

- Availability;
- Equivalent access;
- Confidentiality;
- Data ownership;
- Data reliability.

Requests for information

Rules on requests for information to the Single Points of Contacts include, for instance, the obligation for the submitting authority to carry out a necessity and proportionality test and be ensured that the requested information is available to that other Member State. In addition, the Directive lays down criteria when a request can be considered urgent as well as minimum (formal) requirements for the request in order to allow a rapid and adequate processing. Requests can be submitted by Single Points of Contact or designated Member States' law enforcement authorities.

Time limits

Each Member State must ensure that its Single Point of Contact provides the requested information as soon as possible and in any event within the following time limits, as applicable: (a) eight hours in the case of urgent requests relating to directly accessible information; (b) three calendar days in the case of urgent requests relating to indirectly accessible information; (c) seven calendar days in the case of all other requests.

Deviation from the time limits is possible if a judicial authorisation is needed. In this case, the requested Single Point of Contact must keep the submitting authority updated and provide the requested information as soon as possible after obtaining the judicial authorisation.

Refusal grounds

Regarding the important issue of refusing requests, the Directive first clarifies that refusal should be the exception. Refusal cases are to be specified exhaustively and interpreted restrictively. However, the rules set out in the Directive place an emphasis on the principles of necessity and proportionality, thereby providing safeguards against any misuse of requests for information, including where it would entail manifest breaches of fundamental rights. The Member States, as an expression of their general due diligence, should therefore always verify the compliance of requests submitted to them with the principles of necessity and proportionality and should refuse those requests they find to be non-compliant. Refusal grounds include the following:

- The requested information is unavailable;
- The request does not meet the minimum requirements as to its content (cf. above);
- The required judicial authorisation under national law was refused;
- The requested information constitutes personal data that falls outside the data categories in Annex II.B of Directive 2016/794;
- The requested information has been found to be inaccurate, incomplete or no longer up to date;
- The provision of information would harm or jeopardise important interests;

- The request pertains to:
    - (i) a criminal offence punishable by a maximum term of imprisonment of one year or less under the law of the requested Member State; or
    - (ii) a matter that is not a criminal offence under the law of the requested Member State;
- There is no consent from another Member State or third country which initially provided the data to the requested authority.

Means of information exchange

In order to allow for the necessary flexibility in view of operational needs that might vary in practice, the Directive provides for two other means of exchanging information, in addition to requests for information submitted to the Single Points of Contact. The first one is the unsolicited provision of information by a Single Point of Contact or by a competent law enforcement authority to the Single Point of Contact or a competent law enforcement authority of another Member State without a prior request, i.e. the provision of information on its own initiative.

The second one is the provision of information upon a request for information submitted either by a Single Point of Contact or by a competent law enforcement authority *directly* to a competent law enforcement authority of another Member State. In respect of both means of exchange of information, the Directive sets out only a limited number of minimum requirements.

Language regime and communication channel

The Directive includes an interesting provision on the language to be used for the exchange of information. Member States shall establish and maintain a list of one or more of the languages in which their single contact point is able to exchange information. This list should include English.

The default channel of communication will be Europol's Secure Information Exchange Network Application (SIENA). Following a proposal from the EP, SIENA will also be accessible to front-line officers on mobile phones.

Organisation of Single Points of Contact

Chapter V of the Directive includes harmonised rules on the establishment or designation, tasks and capabilities of Single Points of Contact as well as their organisation, composition and training.

The Single Points of Contact must have access to all information available within their Member State, including by having user-friendly access to all relevant Union and international databases and platforms. It must also be ensured that Single Points of Contact carry out their tasks 24 hours a day, 7 days a week and are provided with qualified staff, appropriate operational tools, technical and financial resources, infrastructure, and capabilities, including for translation, necessary to carry out the tasks under the Directive in an adequate, effective and rapid manner.

Member States must also ensure that the Single Points of Contact deploy and operate a single electronic case management system (CMS). The Directive lays down certain minimum functions and capabilities of such CMS. The CMS is a workflow system allowing Single Points of Contact to manage the exchange of information.

Next steps

The Directive entered into force on 12 June 2023. Member States must transpose the Directive by 12 December 2024. By way of derogation, Member States have time until 12 June 2027 to establish the secure communication channel of the Single Points of Contact with Europol's SIENA.

The Commission shall, by 12 June 2026 and every five years after 12 June 2027, submit a report to the European Parliament and to the Council assessing the implementation of this Directive by the Member States. On 12 June 2027, a first report from the Commission assessing the effectiveness of the Directive is due.

Put in focus

The Directive forms part of the EU Police Cooperation Code package, by which the EU intends to enhance law enforcement cooperation across Member States and to give EU police officers more modern tools for information exchange. The package also contained proposals for automated data exchange for police cooperation ("Prüm II") and for a Council Recommendation on operational police cooperation (→ eucrim 4/2021, 225-226). The legislative procedure regarding the revision of the Prüm framework is still ongoing. The Council Recommendation on "Law Enforcement Cooperation" was adopted in July 2022 (→ eucrim 2/2022, 120).

Directive 2023/977 attempts to remedy flaws encountered by Framework Decision 2006/960. Evaluations showed that the Framework Decision ("the Swedish Initiative") has been scarcely used in practice, in part due to the lack of clarity. One crucial point in practice was unclarity between the Framework Decision and the use of judicial cooperation instruments, such as the Directive regarding the European Investigation Order (EIO). The new Directive on the exchange of information between law enforcement authorities does likely not solve this intricate point either. The question remains unclear of how information is to be exchanged that will subsequently be used as evidence in criminal proceedings. On the one hand, the Directive emphasises that it does not affect Union legal acts on cross-border evidence gathering, such as the EIO Directive and the future Regulation for electronic evidence. On the other hand, it allows the pure consent to the use of already submitted information as evidence in criminal judicial proceedings and vaguely remarks in Recital 14 that this consent *may* be achieved, "where necessary under national law, through the use of instruments regarding judicial cooperation in force between the Member States." It was already unclear under the "Swedish Initiative" under which circumstances and requirements this consent can be given; the Directive rather reinforces the impression that the consent for the use of evidence in judicial proceedings is only a rubberstamp by the authorities of the requested state circumventing the rules of the legislation on judicial cooperation.

The application of the refusal grounds in practice will be another crucial point for the Directive. Interestingly, the Directive words that also the requested law enforcement authority can perform a check of the necessity and proportionality of the information request and not only the requesting authority. This is interesting because such checks by the "executing authority" were to be avoided in other cooperation instruments, such as the European Arrest Warrant.

Unclear remains, however, to which extent the requested authority can deny requests that breach fundamental rights or essential Union values, such as the rule of law. The Directive does not formulate an explicit refusal ground for fundamental rights under the ones listed in Art. 6(1), first sentence. It is only in the subsequent sentence 2 of Art. 6(1) that "Member States shall exercise due diligence in assessing whether the request for information submitted to their Single Point of Contact is in accordance with the requirements set out in Article 4, in particular as to whether there is a manifest breach of fundamental rights."

This formulation is problematic for two reasons: First, Art. 4 of the Directive concerns formal requirements and does not include information on possible fundamental rights breaches in substance. How should the requested authority become aware of fundamental rights infringements? Second, the question arises what means "*manifest* breach". Is it a reference to the ECJ's case law on the European Arrest Warrant (i.e. the so-called *Aranyosi Căldăraru* test)?

In addition, it will be questionable whether the requested law enforcement authority will afford the necessary "due diligence" in practice to probe requests. This is all the more true against the background that the requests have to be executed within short deadlines.

It can only be hoped that the Commission will also take these aspects on safeguards into account in its effectiveness analysis in four years' time.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union