

Law enforcement information exchange

2021/0411(COD) - 15/03/2023 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 507 votes to 99, with 10 abstentions, a legislative resolution on the proposal for a directive of the European Parliament and of the Council on Information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA.

The European Parliament's position adopted at first reading following the ordinary legislative procedure amended the Commission proposal as follows:

Subject matter

This Directive establishes **harmonised rules** for the adequate and rapid exchange of information between the competent law enforcement authorities for the purpose of preventing, detecting or investigating criminal offences.

In particular, this Directive establishes rules on requests for information submitted to the **Single Points of Contact** established or designated by the Member States, in particular on the content of such requests, 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.

Member States may adopt or maintain provisions further facilitating the exchange of information with the competent law enforcement authorities of other Member States for the purpose of preventing, detecting or investigating criminal offences, including by means of bilateral or multilateral arrangements.

All exchanges of information under this Directive should be subject to **five general principles**, namely the principles of availability, equivalent access, confidentiality, data ownership and data reliability.

This Directive does not establish any right to use the information provided in accordance with this Directive as evidence in judicial proceedings. The Member State providing the information may consent to its use as evidence in judicial proceedings.

Activities concerning national security do not fall within the scope of this Directive.

Requests for information to Single Point of Contact

The Directive provides for the possibility for Member States to obtain information by sending a request for information to the Single Point of Contact of other Member States. Member States should ensure that requests for information submitted by their Single Point of Contact and, where their national law so provides, the designated law enforcement authorities to the Single Point of Contact of another Member State comply with the requirements. Member States should submit to the Commission a list of their designated law enforcement authorities. They should inform the Commission where there are changes to that list. The Commission should publish online a compilation of those lists and keep it up to date.

Member States may permit their designated law enforcement authorities not to send, on a case-by-case basis, a copy of a request for information to their Single Point of Contact at the same time as submitting it to the Single Point of Contact of another Member State where it would jeopardise one or more of the following:

- (a) an ongoing highly sensitive investigation for which the processing of information requires an appropriate level of confidentiality;
- (b) terrorism cases not involving emergency or crisis management situations;
- (c) the safety of an individual.

Any request for information submitted to the Single Point of Contact of another Member State should state whether it is urgent and, if so, gives reasons for the urgency. Such requests for information should be considered urgent if:

- (a) they are essential for the prevention of an immediate and serious threat to the public security of a Member State;
- (b) they are necessary in order to prevent an imminent threat to life or the physical integrity of a person;
- (c) they are necessary to adopt a decision that might involve the maintenance of restrictive measures amounting to a deprivation of liberty;
- (d) they present an imminent risk of losing relevance if not provided urgently and is considered important for the prevention, detection or investigation of criminal offences.

Time limits

Member States should ensure that their Single Point of Contact provides the requested information requested 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.

Refusal of requests for information

In exceptional cases, Member State may refuse a request for information submitted to its Single Point of Contact. To ensure the effective functioning of the system created by this Directive in full compliance with the rule of law, those cases should be specified exhaustively and interpreted restrictively. However, the rules set out in this Directive place a strong 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.

List of languages

Member States should 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.

Secure communication channel

Member States should ensure that their Single Point of Contact or their competent law enforcement authorities use Europol's Secure Information Exchange Network Application (SIENA) to send requests for information, to provide information pursuant to such requests or to provide information on its or their own initiative. They should ensure that their Single Point of Contact, and all their competent law enforcement authorities that might be involved in the exchange of information under this Directive, are directly connected to SIENA, including, where appropriate, through mobile devices.

