Council of the European Union

Brussels, 30 May 2022
(OR. fr, en)

9502/22

Interinstitutional File: 2021/0411(COD)

IXIM 137
ENFOPOL 294
JAI 745
CODEC 787
COMIX 261

NOTE

From:	Presidency
To:	Council
No. prev. doc.:	9040/22
No. Cion doc.:	14205/21
Subject:	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 – General approach

I. INTRODUCTION

1. On 9 December 2021, the Commission presented a 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 proposed Directive')[1]. The proposal is part of a new Police Cooperation Code which includes a Recommendation on operational police cooperation[2] and a Regulation on automated data exchange for police cooperation ('Prüm II')[3].

[1] 14205/21.
[2] 14665/21.
[3] 14204/21.

2. The objective of this proposed Directive is to legislate on organisational and procedural aspects of information exchange between law enforcement authorities in the EU with a view to contributing to the effective and efficient exchange of such information, and to help protect a fully functioning and resilient Schengen area.

3. The proposed Directive aims to establish clear and robust common rules on information exchange, common structures and effective management tools for the exchange of information and common practices in the use of the existing communication channel(s) for the exchange of information.

II. WORK IN THE OTHER INSTITUTIONS

4. In the European Parliament, the Committee on Civil Liberties, Justice and Home Affairs (LIBE) has been designated as the competent committee, with Ms Lena Düpont (EPP, DE) appointed rapporteur for this file.

5. The European Data Protection Supervisor issued an opinion on the proposed Directive on 7 March 2022[4].

6. On 18 May 2022, the European Economic and Social Committee adopted an opinion on the Security Union package with regard to several legislative proposals, including the proposed Directive.[5]

III. WORK IN THE COUNCIL PREPARATORY BODIES

7. On 14 December 2021, under the Slovenian Presidency, the proposed Directive and the accompanying impact assessment were presented to the informal meeting of the Working Party on JHA Information Exchange (IXIM).

---

4 https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-directive-information-exchange_en

5 https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/security-union-packageschengen-package

8. Discussions on the proposed Directive continued in the IXIM Working Party under the French Presidency. In total, the proposal was discussed at five IXIM Working Party meetings and two meetings of the JHA counsellors, often on the basis of Presidency compromise proposals.

9. On 11 May 2022, the revised compromise text submitted by the Presidency[6] received broad support. On 12 May 2022, the Presidency transmitted a revised compromise text incorporating the latest amendments supported by delegations[7]. The main elements of the Presidency compromise text relate to the following aspects in particular:

– The scope of the proposed Directive has been clarified. It includes criminal offences defined as 'serious' as well as those which are not covered by that definition. For offences defined as serious, Member States will be obliged to spontaneously communicate the information at their disposal to other Member States where there are objective reasons to believe that such information is relevant to those other Member States for the purposes of that Directive. For criminal offences which are not covered by the definition of 'serious' criminal offence, Member States may spontaneously communicate the information at their disposal to other Member States where there are objective reasons to believe that such information is relevant to those other Member States for the purposes of that Directive;

– A fourth principle has been added to those governing the exchange of information: the principle of data ownership. Thus, where the requested information has initially been obtained from another Member State or a third country, such information may only be provided to the law enforcement authorities of another Member State or Europol with the consent of and according to the conditions imposed on its use by the Member State or third country that initially provided the information, unless that Member State or third country has granted its prior consent to such provision of information;

[6] 8267/3/22 REV 3.
[7] 8267/4/22 REV 4.

– The scope of the definition of ‘law enforcement’ has been clarified. It includes the authorities taking part in joint bodies set up between two or more Member States on the basis of bilateral or multilateral arrangements for the purpose of preventing, detecting or investigating criminal offences. However, agencies or units dealing in particular with national security issues and liaison officers seconded in accordance with Article 47 of the Convention implementing the Schengen Agreement are not covered by this definition of ‘law enforcement’;

– It has been agreed that Member States will be able to designate some of their law enforcement authorities as ‘designated law enforcement authorities’. The latter will, in the same way as a Single Point of Contact, be allowed to send requests for information to the Single Point of Contact of another Member State. The designated law enforcement authorities will have to put their own Single Point of Contact in copy of their requests to the Single Points of Contact of other Member States. However, Member States may decide to allow their law enforcement authorities not to do so on the basis of a list of exceptions for this purpose. This list is used consistently in the text where reference is made to the exceptions to the obligation to put a Single Point of Contact in copy of an exchange of information;

– It has been clarified that Member States will be able to give their consent to the use of information as evidence in judicial proceedings at the time of the provision of such information or afterwards, and may do so, where necessary under their national law, through the use of instruments regarding judicial cooperation in force between the Member States;

– As regards the time limits for the provision of information in response to requests for information addressed to the Single Point of Contact, it has been noted that the time limits provided for in the Presidency compromise have received broad support from delegations. In the context of urgent requests for information, a distinction will be made between information held in a database directly accessible by the Single Point of Contact (time limit of eight hours) and information that the requested Member State can obtain from public authorities or private parties established in that Member State, where permitted by and in accordance with national law, without coercive measures (time limit of three calendar days);

– The list of reasons for refusing requests for information has been slightly broadened. It will be possible to refuse a request for information where the request pertains to a matter that is not an offence under the law of the requested Member State or where it pertains to an offence punishable by a maximum term of imprisonment of one year or less under the law of the requested Member State. In line with the principle of data ownership, a request may also be refused where the information requested has initially been obtained from another Member State or a third country and that Member State or third country has, upon request, not given its consent to the provision of the information;

– It has been clarified that where a law enforcement authority or a Single Point of Contact exchanges information directly with a Single Point of Contact or law enforcement authority of another Member State, it will be expected to send, where appropriate, its own Single Point of Contact and/or the Single Point of Contact of that other Member State a copy of that information, except for the exceptional reasons listed;

– The obligation for Member States to put Europol in copy of exchanges of information has been maintained. However, it will be possible to derogate from this obligation on the basis of a list of exceptions;

– Finally, a list of exceptions has been provided allowing Member States to derogate from the obligation to use SIENA when exchanging information under the Directive.

10. On 25 May 2022, the Permanent Representatives Committee examined the Presidency compromise text. There was broad support for this proposal. The compromise text therefore constitutes a solid basis for reaching a general approach.

IV. CONCLUSIONS

11. In the light of the above, the Council is invited to agree on a general approach on the proposed Directive on the exchange of information between law enforcement authorities of the Member States, as set out in the Annex to this note. The general approach will constitute the mandate for future negotiations with the European Parliament in the context of the ordinary legislative procedure.

ANNEX

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 AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 87(2), point (a), thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Transnational threats involving criminal activities call for a coordinated, targeted and adapted response. While national authorities operating on the ground are on the frontline in the fight against organised crime and terrorism, action at Union level is paramount to ensure efficient and effective cooperation, including as regards the exchange of information. Furthermore, organised crime and terrorism, in particular, are emblematic of the link between internal and external security. Those threats spread across borders and manifest themselves in organised crime and terrorist groups that engage in a wide range of criminal activities.

(2) In an area without internal border controls, police officers in one Member State should have, within the framework of the applicable Union and national law, the possibility to obtain equivalent access to the information available to their colleagues in another Member State. In this regard, law enforcement authorities should cooperate effectively and by default across the Union. Therefore, an essential component of the measures that underpin public security in an interdependent area without internal border controls is police cooperation on the exchange of relevant information for law enforcement purposes. Exchange of information on crime and criminal activities, including terrorism, serves the overall objective of protecting the security of natural persons.

(3) Exchange of information between Member States for the purposes of preventing and detecting criminal offences is regulated by the Convention Implementing the Schengen Agreement of 14 June 1985[8], adopted on 19 June 1990, notably in its Articles 39 and 46. Council Framework Decision 2006/960/JHA[9] partially replaced those provisions and introduced new rules for the exchange of information and intelligence between Member States' law enforcement authorities.

(4) Evaluations, including those carried under Council Regulation (EU) 1053/2013[10], indicated that Framework Decision 2006/960/JHA is not sufficiently clear and does not ensure adequate and rapid exchange of relevant information between Member States. Evaluations also indicated that that Framework Decision is scarcely used in practice, in part due to the lack of clarity experienced in practice between the scope of the Convention Implementing the Schengen Agreement and of that Framework Decision.

---

8 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (OJ L 239, 22.9.2000, p. 19).

9 Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (*OJ L 386, 29.12.2006, p. 89).*

10 Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen (OJ L 295*, 6.11.2013, p. 27).*

(5) Therefore, the existing legal framework consisting of the relevant provisions of the Convention Implementing the Schengen Agreement and Framework Decision 2006/960/JHA should be updated and replaced, so as to facilitate and ensure, through the establishment of clear and harmonised rules, the adequate and rapid exchange of information between the competent law enforcement authorities of different Member States.

(6) In particular, the discrepancies between the relevant provisions of the Convention Implementing the Schengen Agreement and Framework Decision 2006/960/JHA should be addressed by covering information exchanges for the purpose of preventing, detecting or investigating criminal offences, thereby fully superseding, insofar as such exchanges are concerned, Articles 39 and 46 of that Convention and hence providing the necessary legal certainty. In addition, the relevant rules should be simplified and clarified, so as to facilitate their effective application in practice.

(7) It is necessary to lay down rules governing the cross-cutting aspects of such information exchange between Member States***, including information obtained in criminal intelligence operations. This should include the exchange of information through Police and Customs Cooperation Centres set up between two or more Member States on the basis of bilateral or multilateral arrangements for the purpose of preventing, detecting or investigating criminal offences. On the other hand, this should not include bilateral exchange of information with Third States***. The rules of this Directive should not affect the application of rules of Union law on specific systems or frameworks for such exchanges, such as under Regulations (EU) 2018/1860[11], (EU) 2018/1861[12], (EU) 2018/1862[13], and (EU) 2016/794[14] of the European Parliament and of the Council, Directives (EU) 2016/681[15] and 2019/1153[16] of the European Parliament and of the Council, and Council Decisions 2008/615/JHA[17] and 2008/616/JHA[18].

---

11 Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals (OJ L 312, 7.12.2018, *p. 1)*.

12 Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation No 1987/2006 (OJ L 312, 7.12.2018, p. 14).

13 Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

14 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (*OJ L 135, 24.5.2016, p. 53)*.

15 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (*OJ L 119, 4.5.2016, p. 132).*

16 Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (*OJ L 186, 11.7.2019, p. 122).*

17 Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1).

18 Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12). A proposal for a Regulation on automated data exchange for police cooperation ("Prüm II"), intends to repeal parts of those Council Decisions.

This Directive is without prejudice to the provisions of the Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations (Naples II).

(7a) Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security should not be considered to be activities falling within the scope of this Directive.

(8) This Directive does not govern the provision and use of information as evidence in judicial proceedings. In particular, it should not be understood as establishing a right to use the information provided under this Directive as evidence and, consequently, it leaves unaffected any requirement provided for in the applicable law to obtain the consent from the Member State providing the information for such use. This Directive leaves acts of Union law on evidence, such as Regulation (EU) …/…[19] [*on European Production and Preservation Orders for electronic evidence in criminal matters*] and Directive (EU) …/…[20] [*laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*], unaffected. ***Consequently, Member States may give their consent for the use of information as evidence in judicial proceedings at the time of the provision of the information or afterwards, including where necessary under national law, through the use of instruments regarding judicial cooperation in force between the Member States.***

[19] Regulation proposal, COM/2018/225 final - 2018/0108 (COD).
[20] Directive proposal, COM/2018/226 final - 2018/0107 (COD).

(9) All exchanges of information under this Directive should be subject to ***four*** [...] general principles, namely those of availability, equivalent access***,*** [...] confidentiality ***and data ownership***. While those principles are without prejudice to the more specific provisions of this Directive, they should guide its interpretation and application where relevant. For example, the principle of availability should be understood as indicating that relevant information available to the Single Point of Contact or the law enforcement authorities of one Member State should also be available, to the largest extent possible, to those of other Member States. However, the principle should not affect the application, where justified, of specific provisions of this Directive restricting the availability of information, such as those on the grounds for refusal of requests for information and judicial authorisation***, as well as the obligation to have the consent of the State which initially provided the information to share it***. In addition, pursuant to the principle of equivalent access, the access of the Single Point of Contact and the law enforcement authorities of other Member States to relevant information should be substantially the same as, and thus be neither stricter nor less strict than, the access of those of one and the same Member State, subject to the Directive's more specific provisions.

(9a) The concept of available information on which the Directive is based includes both information directly accessible and indirectly accessible to law enforcement authorities. Directly accessible information refers to all information that is held in a database directly accessible by the Single Point of Contact or the law enforcement authorities of the requested Member State, whether or not it was previously obtained by coercive measures. On the other hand, indirectly accessible information requires action by the Single Point of Contact or the law enforcement authorities of the requested Member State to obtain it. This action should not include coercive measures. Each Member State should provide its list of directly accessible information and its list of indirectly accessible information to the General Secretariat of the Council to be included in the "National Fact Sheets" appended to the Council document "Manual on Law Enforcement Information Exchange".

(10) In order to achieve the objective to facilitate and ensure the adequate and rapid exchange of information between Member States, provision should be made for obtaining such information by addressing a request for information to the Single Point of Contact of the other Member State concerned, in accordance with certain clear, simplified and harmonised requirements. Concerning the content of such requests for information, it should in particular be specified, in an exhaustive and sufficiently detailed manner and without prejudice to the need for a case-by-case assessment, when they are to be considered as urgent and which explanations they are to contain as minimum.

(11) Whilst the Single Points of Contact of each Member State should in any event have the possibility to submit requests for information to the Single Point of Contact of another Member State, in the interest of flexibility, Member States should be allowed to decide that, in addition, ***some of*** their law enforcement authorities ***involved in European cooperation*** may also submit such requests ***to the Single Points of Contact of other Member States***. ***The list of these designated law enforcement authorities should be updated and provided by each Member State to the Commission and to the General Secretariat of the Council to be included in the "National Fact Sheets" appended to the Council document "Manual on Law Enforcement Information Exchange"***. In order for Single Points of Contact to be able to perform their coordinating functions under this Directive, it is however necessary that, where a Member State takes such a decision, its Single Point of Contact is made aware of all such outgoing requests, as well as of any communications relating thereto, by always being put in copy.

(12) Time limits are necessary to ensure rapid processing of requests for information submitted to a Single Point of Contact. Such time limits should be clear and proportionate and take into account whether the request for information is urgent and whether ***the information is directly or indirectly accessible to the law enforcement authorities*** [...]. In order to ensure compliance with the applicable time limits whilst nonetheless allowing for a degree of flexibility where objectively justified, it is necessary to allow, on an exceptional basis, for deviations only where, and in as far as, the competent judicial authority of the requested Member State needs additional time to decide on granting the necessary judicial authorisation. Such a need could arise, for example, because of the broad scope or the complexity of the matters raised by the request for information. ***In order to limit the risks of losing the opportunity to proceed to critical actions in specific cases, information should be provided to the requesting Member State as soon as the information is held by the Single Point of Contact even if that information is only part of the overall information available that is relevant to the request. The rest of the information should be provided afterwards.***

(13) In exceptional cases, it may be objectively justified for a Member State to refuse a request for information submitted to a Single Point of Contact. In order to ensure the effective functioning of the system created by this Directive, those cases should be exhaustively specified and interpreted restrictively. When only parts of the information concerned by such a request for information relate to the reasons for refusing the request, the remaining information is to be provided within the time limits set by this Directive. Provision should be made for the possibility to ask for clarifications, which should suspend the applicable time limits. However, such possibility should only exist where the clarifications are objectively necessary and proportionate, in that the request for information would otherwise have to be refused for one of the reasons listed in this Directive. In the interest of effective cooperation, it should remain possible to request necessary clarifications also in other situations, without this however leading to suspension of the time limits.

(14) In order to allow for the necessary flexibility in view of operational needs that may vary in practice, provision should be made 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 spontaneous provision of information, that is, on the own initiative of either the Single Point of Contact or the law enforcement authorities without a prior request. The second one is the provision of information upon requests for information submitted either by Single Points of Contact or by law enforcement authorities not to the Single Point of Contact, but rather directly to the law enforcement authorities of another Member State. In respect of both means, only a limited number of minimum requirements should be set, in particular on keeping the Single Points of Contact informed and, as regards own-initiative provision of information, the situations in which information is to be provided and the language to be used.

(15) The requirement of a prior judicial authorisation for the provision of information can be an important safeguard. The Member States' legal systems are different in this respect and this Directive should not be understood as affecting such requirements established under national law, other than subjecting them to the condition that domestic exchanges and exchanges between Member States are treated in an equivalent manner, both on the substance and procedurally. Furthermore, in order to keep any delays and complications relating to the application of such a requirement to a minimum, the Single Point of Contact or the law enforcement authorities, as applicable, of the Member State of the competent judicial authority should take all practical and legal steps, where relevant in cooperation with the Single Point of Contact or the law enforcement authority of another Member State that requested the information, to obtain the judicial authorisation as soon as possible. ***Although the legal basis of the Directive is limited to law enforcement cooperation under Article 87(2)(a) of the Treaty on the Functioning of the European Union, this does not prevent judicial authorities from being concerned by some of the provisions of this Directive.***

(16) It is particularly important that the protection of personal data, in accordance with Union law, is ensured in connection to all exchanges of information under this Directive. To that aim, the rules of this Directive should be aligned with Directive (EU) 2016/680 of the European Parliament and of the Council[21]. In particular, it should be specified that any personal data exchanged by Single Points of Contacts and law enforcement authorities is to remain limited to the categories of data listed in Section B point 2, of Annex II to Regulation (EU) 2016/794 of the European Parliament and of the Council[22]. Furthermore, as far as possible, any such personal data should be distinguished according to their degree of accuracy and reliability, whereby facts should be distinguished from personal assessments, in order to ensure both the protection of individuals and the quality and reliability of the information exchanged. If it appears that the personal data are incorrect, they should be rectified or erased without delay. Such rectification or erasure, as well as any other processing of personal data in connection to the activities under this Directive, should be carried out in compliance with the applicable rules of Union law, in particular Directive (EU) 2016/680 and Regulation (EU) 2016/679 of the European Parliament and of the Council[23], which rules this Directive leaves unaffected.

---

21 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 (OJ L 119 4.5.2016, p. 89).

22 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (*OJ L 135, 24.5.2016, p. 53).*

23 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) (OJ L 119 4.5.2016, p. 1).

(17) In order to allow for adequate and rapid provision of information by Single Points of Contact, either upon request or on their own initiative, it is important that the relevant officials of the Member States concerned understand each other. Language barriers often hamper the cross-border exchange of information. For this reason, rules should be established on the use of languages in which requests for information submitted to the Single Points of Contact, the information to be provided by Single Points of Contact as well as any other communications relating thereto, such as on refusals and clarifications, are to be provided. Those rules should strike a balance between, on the one hand, respecting the linguistic diversity within the Union and keeping costs of translation as limited as possible and, on the other hand, operational needs associated with adequate and rapid exchanges of information across borders. Therefore, Member States should establish a list containing one or more [...] languages [...]of their choice, but containing also one language that is broadly understood and used in practice, namely, English. ***This list of languages should be updated and provided by each Member State to the Commission and to to the General Secretariat of the Council to be included in the "National Fact Sheets" appended to the Council document "Manual on Law Enforcement Information Exchange".***

(18) The further development of the European Union Agency for Law Enforcement Cooperation (Europol) as the Union's criminal information hub is a priority. That is why, when information or any related communications are exchanged, irrespective of whether that is done pursuant to a request for information submitted to a Single Point of Contact or law enforcement authority, or on their own-imitative, a copy should be sent to Europol, however only insofar as it concerns offences falling within the scope of the objectives of Europol. ***This provision goes further than the Regulation (EU) 2016/794 of the European Parliament and of the Council and reinforces the provisions of its Article 7(6)(a), which leaves it to the discretion of the Member State to decide whether information should be sent to the Agency.*** In practice, this can be done through the ticking by default of the corresponding SIENA box. ***In certain cases where the transmission of information to Europol could jeopardise national security, an ongoing investigation or the safety of an individual, or disclosing the information would jeopardise the data ownership principle, the Single Points of Contact and the law enforcement authorities should be able to derogate from this mandatory copying, which justifies the establishment of a list of exceptions in line with Article 7(7) of the Regulation (EU) 2016/794 of the European Parliament and of the Council. This provision is without prejudice to Articles 18 and 19 of the Regulation (EU) 2016/794 of the European Parliament and of the Council, pertaining to the determination of the purpose of, and restrictions on, the processing of information by Europol.***

(19) The proliferation of communication channels used for the transmission of law enforcement information between Member States [...] should be remedied, as it hinders the adequate and rapid exchange of such information. Therefore, the use of the secure information exchange network application called SIENA, managed by Europol in accordance with Regulation (EU) 2016/794, should be made mandatory for all such transmissions and communications under this Directive, including the sending of requests for information submitted to Single Points of Contact and directly to law enforcement authorities, the provision of information upon such requests and on their own initiative, communications on refusals and clarifications, as well as copies to Single Points of Contact and Europol. ***This should not apply to internal exchanges of information within a Member State.*** To that aim, all Single Points of Contact, as well as all law enforcement authorities that may be involved in such exchanges, should be directly connected to SIENA. In this regard, a transition period should be provided for, however, in order to allow for the full roll-out of SIENA. ***In addition, in order to take into account the operational reality and not to hamper good cooperation between law enforcement authorities, a list of exceptions has been established to address cases where the choice of another secure communication channel is justified and promotes the exchange of information.***

(20) In order to simplify, facilitate and better manage information flows, Member States should each establish [...] one Single Point of Contact competent for coordinating information exchanges under this Directive. ***Each Member State, after establihsing its Single Point of Contact, should provide that information to the Commission for subsequent publication and should update that information where necessary. Each Member State should provide the same information to the General Secretariat of the Council to be included in the "National Fact Sheets" appended to the Council document "Manual on Law Enforcement Information Exchange".*** The Single Points of Contact should, in particular, contribute to mitigating the fragmentation of the law enforcement authorities' landscape, specifically in relation to information flows, in response to the growing need to jointly tackle cross-border crime, such as drug trafficking and terrorism. For the Single Points of Contact to be able to effectively fulfil their coordinating functions in respect of the cross-border exchange of information for law enforcement purposes under this Directive, they should be assigned a number of specific, minimum tasks and also have certain minimum capabilities.

(21) Those capabilities of the Single Points of Contact should include having access to all information available within its own Member State ***whether this information is directly or indirectly accessible to the law enforcement authorities in accordance with recital (9a)***, including by having user-friendly access to all relevant Union and international databases and platforms, in accordance with the modalities specified in the applicable Union and national law. In order to be able to meet the requirements of this Directive, especially those on the time limits, the Single Points of Contact should be provided with adequate resources, including adequate translation capabilities, and function around the clock. In that regard, having a front desk that is able to screen, process and channel incoming requests for information may increase their efficiency and effectiveness. Those capabilities should also include having at their disposition, at all times, judicial authorities competent to grant necessary judicial authorisations. In practice, this can be done, for example, by ensuring the physical presence or the functional availability of such judicial authorities, either within the premises of the Single Point of Contact or directly available on call.

(22) In order for them to be able to effectively perform their coordinating functions under this Directive, the Single Points of Contact should be composed of representatives of national law enforcement authorities whose involvement is necessary for the adequate and rapid exchange of information under this Directive. While it is for each Member State to decide on the precise organisation and composition needed to meet that requirement, such representatives may include police, customs and other law enforcement authorities competent for preventing, detecting or investigating criminal offences, as well as possible contact points for the regional and bilateral offices, such as liaison officers and attachés seconded or posted in other Member States and relevant Union law enforcement agencies, such as Europol. However, in the interest of effective coordination, at minimum, the Single Points of Contact should be composed of representatives of the Europol national unit, the SIRENE Bureau[...] and the Interpol National Central Bureau, as established under the relevant legislation and notwithstanding this Directive not being applicable to information exchanges specifically regulated by such Union legislation.

(23) The deployment and operation of an electronic single Case Management System having certain minimum functions and capabilities by the Single Points of Contact is necessary to allow them to carry out their tasks under this Directive in an effective and efficient manner, in particular as regards information management. ***The universal message format (UMF) standard should be used in the development of the Case Management System. Member States' authorities and Europol are encouraged to use the UMF standard, which should serve as a standard for structured, cross-border information exchange between information systems, authorities or organisations in the field of Justice and Home Affairs.***

(24) To enable the necessary monitoring and evaluation of the application of this Directive, Member States should be required to collect and annually provide to the Commission certain data. This requirement is necessary, in particular, to remedy the lack of comparable data quantifying relevant information exchanges and also facilitates the reporting obligation of the Commission. ***Required data should be automatically generated by the Case Management System and SIENA.***

(25) The cross-border nature of crime and terrorism requires Member States to rely on one another to tackle such criminal offences. Adequate and rapid information flows between relevant law enforcement authorities and to Europol cannot be sufficiently achieved by the Member States acting alone. Due to the scale and effects of the action, this can be better achieved at Union level through the establishment of common rules on the exchange of information. Thus, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(26) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Directive and is not bound by it or subject to its application. Given that this Directive builds upon the Schengen acquis, Denmark should, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Directive whether it will implement it in its national law.

(27) This Directive constitutes a development of the provisions of the Schengen *acquis* in which Ireland takes part, in accordance with Council Decision 2002/192/EC[24]; Ireland is therefore taking part in the adoption of this Directive and is bound by it.

(28) As regards Iceland and Norway, this Directive constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis*[25] which fall within the area referred to in Article 1, point H of Council Decision 1999/437/EC[26].

---

[24] Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen acquis (OJ L 64, 7.3.2002).

[25] OJ L 176, 10.7.1999, p. 36.

[26] Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis (OJ L 176, 10.7.1999).

(29) As regards Switzerland, this Directive constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[27] which fall within the area referred to in Article 1, point H of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC[28] and with Article 3 of Council Decision 2008/149/JHA[29].

[27] OJ L 53, 27.2.2008, p. 52.

[28] Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis (OJ L 53, 27.2.2008).

[29] Council Decision 2008/149/JHA of 28 January 2008 on the conclusion on behalf of the European Union of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis (OJ L 53, 27.2.2008).

(30) As regards Liechtenstein, this Directive constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[30] which fall within the area referred to in Article 1, point H of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU[31] and with Article 3 of Council Decision 2011/349/EU[32],

HAVE ADOPTED THIS DIRECTIVE:

---

[30] OJ L 160, 18.6.2011, p. 21.

[31] Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011).

[32] Council Decision 2011/349/EU of 7 March 2011 on the conclusion on behalf of the European Union of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis relating in particular to judicial cooperation in criminal matters and police cooperation (OJ L 160, 18.6.2011).

Chapter I

General provisions

Article 1

Subject matter and scope

1. This Directive establishes rules for the exchange of information between the law enforcement authorities of the Member States [...] for the purpose***s*** of preventing, detecting or investigating criminal offences.

   In particular, this Directive establishes rules on:

   (a) requests for information submitted to the Single Points of Contact established [...] by the Member States, in particular on the content of such requests, ***the provision of information pursuant to such requests,*** mandatory time limits for providing the requested information, ***and the*** reasons for refusals of such requests [...];

   (b) the own-initiative provision of relevant information to Single Points of Contact or to the law enforcement authorities of other Member States, in particular the situations and the manner in which such information is to be provided;

   (c) the channel of communication to be used for [...] exchanges of information ***under this Directive*** and the information to be provided to the Single Points of Contact in relation to exchanges of information directly between the law enforcement authorities of the Member States;

   (d) the establishment, tasks, composition and capabilities of the Single Point of Contact, including on the deployment of a single electronic Case Management System ***providing the functions and capabilities set out in Article 16(1)*** for the [...] tasks ***set out in Article 14(2)***.

2. This Directive shall not apply to exchanges of information between the law enforcement authorities of the Member States for the purpose of preventing, detecting or investigating criminal offences that are specifically regulated by other acts of Union law. ***Without prejudice to their obligations under this Directive and other acts of Union law, Member States may adopt or maintain provisions further facilitating the exchange of information with the law enforcement authorities of other Member States for the purposes of preventing, detecting or investigating criminal offences, including by means of bilateral or multilateral arrangements concluded by the Member States.***

3. This Directive does 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 law enforcement authorities of other Member States*** [...];

   (c) provide information to the law enforcement authorities of other Member States to be used as evidence in judicial proceedings**.**

4. 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 give consent for its use as evidence in judicial proceedings, including where necessary under national law, through the use of instruments regarding judicial cooperation in force between the Member States.***

Article 2

Definitions

For the purpose of this Directive:

(1) 'law enforcement authority' means any authority of the Member States competent under national law for the purpose of preventing, detecting or investigating criminal offences***, including such authorities that take part in joint entities set up between two or more Member States on the basis of bilateral or multilateral arrangements for the purpose of preventing, detecting or investigating criminal offences. Agencies or units dealing especially with national security issues and liaison officers seconded pursuant to Art. 47 of the CISA are not covered by this definition of law enforcement authority***;

(1a) 'designated law enforcement authority' means a law enforcement authority that is authorised to submit requests for information to the Single Points of Contact of other Member States in accordance with Article 4(1);

(2) '***serious*** criminal offences' means any of the following:

(a) offences referred to in Article 2(2) of Council Framework Decision 2002/584/JHA[33];

(b) offences referred to in Article 3(1) and (2) of Regulation (EU) 2016/794;

(c) [...]

[33] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002*, p. 1)*.

(3) 'information' means any content concerning one or more natural ***or legal*** persons, facts or circumstances relevant to law enforcement authorities ***for the purpose of*** [...] exercis***ing***[...] their tasks under national law of preventing, detecting or investigating criminal offences ***or criminal intelligence***;

(4) 'available' information means information that is either held ***in a database directly accessible*** by the Single Point of Contact or the law enforcement authorities of the requested Member State ***(direct access)***, or information that those Single Points of Contact or those law enforcement authorities can obtain from other public authorities or from private parties established in that Member State***, where permitted by and in accordance with national law,*** without coercive measures ***(indirect access)***;

(5) 'SIENA' means the secure information exchange network application, managed ***and developed*** by Europol, aimed at facilitating the exchange of information between Member States and Europol;

(6) 'personal data' means personal data as defined in Article ***3*** [...], point (1) of [...] ***Directive*** (EU) 2016/6***80*** [...]**;**

(7) 'requesting Member State' means the Member State whose Single Point of Contact or designated law enforcement authority submits a request for information in accordance with Article 4;

(8) 'requested Member State' means the Member State whose Single Point of Contact receives a request for information in accordance with Article 4.

Article 3

Principles of information exchange

Member States shall, in connection to all exchanges of information under this Directive, ensure that:

(a) [...] information available to the***ir*** Single Point of Contact or [...] law enforcement authorities [...] ***can be*** [...] provided to the Single Point of Contact or the law enforcement authorities of other Member States ***in accordance with this Directive*** ('principle of availability');

(b) the conditions for requesting information from the Single Point**s** of Contact [...] of other Member States, and those for providing information to the Single Points of Contact and the ***designated*** law enforcement authorities of other Member States, are equivalent to those applicable for requesting and providing similar information [...] ***at national level*** ('principle of equivalent access');

(c) information provided to the Single Point**s** of Contact or the law enforcement authorities of [...]other Member State**s** that is marked as confidential is protected by th***em*** [...] in accordance with the requirements set out in the national law of that Member State offering a similar level of confidentiality ('principle of confidentiality').

(d) where the requested information has initially been obtained from another Member State or a third country, such information may only be provided to the law enforcement authority of another Member State or Europol with the consent of and according to the conditions imposed on its use by the Member State or third country that initially provided the information, unless that Member State or third country has granted its prior consent to such provision of information ('principle of data ownership').

Chapter II

Exchanges of information through Single Points of Contact

Article 4

Requests for information to the Single Point of Contact

1. Member States shall ensure that ***the request for information that*** their Single Point of Contact and, where they have so decided, the[...] ***designated*** law enforcement authorities submit [...] to the Single Point[...] of Contact of ***an***other Member State[...] ***comply*** with the conditions set out in paragraphs 2 to 5.

Member States shall notify the Commission with the list of law enforcement authorities designated at national level to submit requests for information directly to the Single Points of Contact of other Member States. They shall update that information where necessary.

[...] Member State***s*** [...] shall ensure that th[...]e***ir designated law enforcement*** authorities send, at the same time as submitting such requests, a copy of those requests[...] to the Single Point of Contact of that Member State. ***For the exceptional reasons set out in paragraph 1a, Member States may decide to permit their designated law enforcement authorities not to send such a copy.***

1a. Member States may decide to permit their designated law enforcement authorities not to send, at the same time as submitting requests in accordance with paragraph 1, a copy of those requests to the Single Point of Contact of that Member State in the following cases:

(a) highly sensitive investigations which need an appropriate level of confidentiality for the processing of their information, where the investigation could be jeopardised;

(b) terrorism cases not involving emergency or crisis management situations;

(c) protection of individuals whose safety may be in jeopardy.

2. Requests for information to the Single Point of Contact of another Member State shall be submitted only where there are objective reasons to believe that:

(a) the requested information is necessary and proportionate to achieve the purpose referred to in Article 1(1);

(b) the requested information is available to [...] th***at*** [...] Member State***, as defined in Article 2(4)***.

3. Any request for information to the Single Point of Contact of another Member State shall specify whether or not it is urgent.

Those requests for information shall be considered urgent if, having regard to all relevant facts and circumstances of the case at hand, there are objective reasons to believe that the requested information is one or more of the following:

(a) essential for the prevention of an immediate and serious threat to the public security of a Member State;

(b) necessary in order to protect ***the life or physical integrity of*** a person[...] which are at imminent risk;

(c) necessary to adopt a decision that may involve the maintenance of restrictive measures amounting to a deprivation of liberty;

(d) at imminent risk of losing relevance if not provided urgently.

4. Requests for information to the Single Point of Contact of another Member State shall contain all necessary explanations to allow for their adequate and rapid processing in accordance with this Directive, including at least the following:

(a) a specification of the requested information that is as detailed as reasonably possible under the given circumstances;

(b) a description of the purpose for which the information is requested ***including a description of the facts and indication of the underlying offence***;

(c) the objective reasons according to which it is believed that the requested information is available to [...] th***at***[...] Member State ***as defined in Article 2(4)***;

(d) an explanation of the connection between the purpose and [...] ***any*** person or ***subject*** [...] to wh[...]***ich*** the information relates, where applicable;

(e) the reasons for which the request is considered urgent, where applicable***;***

(f) restrictions on the use of the information contained in the request for purposes other than those for which it has been submitted.

5. Requests for information to the Single Point of Contact of another Member State shall be submitted in one of the languages included in the list established by the requested Member State and published in accordance with Article 11.

Article 5

Provision of information pursuant to requests to the Single Point of Contact

1. Subject to paragraph 2 of this Article and to Article 6(3), Member States shall ensure that their Single Point of Contact provides the information requested in accordance with Article 4 as soon as possible and [...] within the following time limits, as applicable:

   (a) eight hours, for urgent requests relating to information that is [...] ***held in a database directly accessible by the Single Point of Contact or*** the law enforcement authorities of the requested Member State ***(direct access) according to Article 2(4)*** [...];

   (b) three calendar days, for urgent requests relating to information that ***the Single Point of Contact or*** [...] the law enforcement authorities of the requested Member State ***can obtain from other public authorities or from private parties established in that Member State, where permitted by and in accordance with national law, without coercive measures (indirect access)*** [...];

   (c) seven calendar days, for all ***other*** requests [...].

   The time [...] ***limits*** laid down in the first subparagraph shall commence at the moment of the reception of the request for information.

2. Where under its national law in accordance with Article 9 the requested information is available only after having obtained a judicial authorisation, the requested Member State may deviate from the time limits [...] ***determined in*** paragraph 1 insofar as necessary for obtaining such authorisation.

In such cases, Member States shall ensure that their Single Point of Contact does both of the following:

(i) immediately inform the [...] requesting Member State of the expected delay, specifying the length of the expected delay and the reasons therefore;

(ii) subsequently keep it updated and provide the requested information as soon as possible after obtaining the judicial authorisation.

3. Member States shall ensure that their Single Point of Contact provides the information requested in accordance with Article 4 to the [...] requesting Member State*,* in the language in which that request for information was submitted in accordance with Article 4(5).

Member States shall ensure that, where their Single Point of Contact provides the requested information to the ***designated*** law enforcement authority of the requesting Member State, it also sends, at the same time, a copy of the information to the Single Point of Contact of that Member State.

4. For the exceptional reasons listed in Article 4(1a), Member States may decide to permit their Single Point of Contact not to send, at the same time as providing information to the designated law enforcement authorities of another Member State in accordance with this Article, a copy of that information to the Single Point of Contact of that Member State.

5. Member States shall ensure that, if the requested information is not available to the Single Point of Contact and the law enforcement authorities of the requested Member State, their Single Point of Contact inform the requesting Member State.

Article 6

Refusals of requests for information

1. ***Without prejudice to Article 3(b),*** Member States shall ensure that their Single Point of Contact only refuses to provide the information requested in accordance with Article 4 insofar as any of the following reasons applies:

(a) [...]

(b) the request for information does not meet the requirements set out in Article 4;

(c) the judicial authorisation required under the national law of the requested Member State in accordance with Article 9 was refused;

(d) [...]

(e) there are objective reasons to believe that the provision of the requested information would:

(i) be contrary to ***or would harm*** the essential interests of the ***national*** security of the requested Member State;

(ii) jeopardise [...] an ongoing investigation of a criminal offence; or;

(iii) ***jeopardise the safety of an individual*** [...].

(f) the request pertains to an offence punishable by a maximum term of imprisonment of one year or less under the law of the requested Member State or the request pertains to a matter that is not an offence under the law of that Member State;

(g) the requested information has initially been obtained from another Member State or a third country and that Member State or third country has, upon request, not given its consent to the provision of the information.

Any refusal shall only affect the part of the requested information to which the reasons set out in the first subparagraph relate and shall, where applicable, leave the obligation to provide the other parts of the information in accordance with this Directive unaffected.

2. Member States shall ensure that their Single Point of Contact informs [...] the requesting Member State of the refusal, specifying the reasons for the refusal, within the time limits provided for in Article 5(1).

3. Member States shall ensure that their Single Point of Contact immediately requests ***from the requesting Member State*** additional clarifications needed to process a request for information that otherwise would have to be refused [...].

The time limits referred to in Article 5(1) shall be suspended from the moment that the [...] requesting Member State receives the request for clarifications, until the moment that the Single Point of Contact of the requested Member State receives the clarifications.

4. The refusals, reasons for the refusals, requests for clarifications and clarifications referred to in paragraphs 3 and 4, as well as any other communications relating to the requests for information to the Single Point of Contact of another Member State, shall be transmitted in the language in which that request was submitted in accordance with Article 4(5).

Chapter III

Other exchanges of information

Article 7

Own-initiative provision of information

0. Member States may provide on their own initiative, through their Single Point of Contact or through their law enforcement authorities, information available to them to the Single Points of Contact or to the law enforcement authorities of other Member States, where there are objective reasons to believe that such information could be relevant to that Member State for the purposes referred to in Article 1(1).

1. Member States shall ensure that their Single Point of Contact or their law enforcement authorities provide, on their own initiative, [...] information available to them to the Single Points of Contact or to the law enforcement authorities of other Member States, where there are objective reasons to believe that such information could be relevant to that Member State for the purpose***s of preventing, detecting or investigating serious criminal offences as defined in Article 2(2)*** **[...]**. However, no such obligation shall exist insofar as the reasons referred to in points (c)[...] or (e) of Article 6(1) apply in respect of such information.

2. Member States shall ensure that, where their Single Point of Contact or their law enforcement authorities provide information on their own-initiative ***to the Single Point of Contact of the other Member State*** in accordance with paragraph ***0 and*** 1, they do so in one of the languages included in the list established by the ***receiving*** [...] Member State and published in accordance with Article 11.

Member States shall ensure that, where their Single Point of Contact [...] provide***s*** such information to the law enforcement authority of another Member State, they also send, at the same time, a copy of that information to the Single Point of Contact of that other Member State. ***Member States shall ensure that, where their law enforcement authorities provide such information to the Single Point of Contact or to the law enforcement authority of another Member State, they also send, at the same time, a copy of that information to their own Single Point of Contact or to the Single Point of Contact of that other Member State, as appropriate.***

2a. For the exceptional reasons listed in Article 4(1a), Member States may decide to permit their law enforcement authorities not to send, at the same time as providing information to the Single Point of Contact or the law enforcement authorities of another Member State in accordance with this Article, a copy of that information to their own Single Point of Contact or to the Single Point of Contact of that Member State.

Article 8

Exchanges of information upon requests submitted directly to law enforcement authorities

1. Member States shall ensure that, where ***their*** Single Points of Contact [...] submit requests for information directly to the law enforcement authorities of another Member State, [...] ***they provide, at the same time,*** a copy [...] ***of those requests*** to the Single Point of Contact of that other Member State. ***Member States shall ensure that, where their law enforcement authorities provide information pursuant to such requests, they provide, at the same time, a copy of that information to their own Single Point of Contact.***

1a. ***For the exceptional reasons listed in Article 4(1a), Member States may decide to permit their Single Point of Contact not to send, at the same time as requesting information to the law enforcement authorities of another Member State in accordance with paragraph 1, a copy of that request to the Single Point of Contact of that other Member State. For the exceptional reasons listed in Article 4(1a), Member States may decide to permit their law enforcement authorities not to send, at the same time as providing information to the Single Point of Contact of another Member State in accordance with paragraph 1, a copy of that information to their own Single Point of Contact.***

2. ***Member States shall ensure that, where their law enforcement authorities submit requests for information or provide information pursuant to such requests directly to the law enforcement authorities of another Member State, they provide, at the same time, a copy of that request or that information*** [...] to the***ir own*** Single Point of Contact [...] ***as well as to the Single Point of Contact of that other Member State***.

2a. For the exceptional reasons listed in Article 4(1a), Member States may decide to permit their law enforcement authorities not to send, at the same time as requesting or providing information to the law enforcement authorities of another Member State in accordance with paragraph 2, a copy of that request or that information to their own Single Point of Contact or to the Single Point of Contact of that other Member State.

Chapter IV

Additional rules on the provision of information under Chapters II and III

Article 9

Judicial authorisation

1. Member States shall not require any judicial authorisation for the provision of information to the Single Points of Contact or ***to the*** law enforcement authority of another Member State under Chapters II and III, where no such requirement applies in respect of similar provision of information [...] ***at national level***.

2. Member States shall ensure that, where their national law requires a judicial authorisation for the provision of information to [...] another Member State in accordance with paragraph 1, their Single Point[...] of Contact or their law enforcement authorities immediately take all necessary steps, in accordance with their national law, to obtain such judicial authorisation as soon as possible.

3. The requests for judicial authorisation referred to in paragraph 1 shall be assessed and decided upon in accordance with the national law of the Member State of the competent judicial authority.

Article 10

Additional rules for information constituting personal data

Member States shall ensure that, where their Single Point of Contact or their law enforcement authorities provide information under Chapters II and III that constitutes personal data:

(i) the categories of personal data provided remain limited to those ***necessary and proportionate to achieve the purpose of the request,*** listed in Section B, point 2, of Annex II to Regulation (EU) 2016/794;

(ii) their Single Point of Contact or their law enforcement authorities also provide, at the same time and insofar as possible, the necessary elements enabling the Single Point of Contact or the law enforcement authority of the other Member State to assess the degree of accuracy, completeness and reliability of the personal data, as well as the extent to which the personal data are up to date.

Article 11

List of languages

1. Member States shall establish and keep up to date a list with one or more of the [...] languages [...] in which their Single Point of Contact is able to ***exchange information*** [...] . That list shall include English.

2. Member States shall provide those lists, as well as any updates thereof, to the Commission. [...]

Article 12

Provision of information to Europol

1. Member States shall ensure that, where their Single Point of Contact or their law enforcement authorities send requests for information, provide information pursuant to such requests, provide information on their own initiative [...] under Chapters II and III, they also send, at the same time, a copy thereof to Europol, insofar as the information to which the communication relates concerns offences falling within the scope of the objectives of Europol in accordance with Regulation (EU) 2016/794.

2. ***Member States may decide not to provide or to defer the provision of a copy to Europol if such provision would:***

(a) ***be contrary to or would harm the essential interests of the national security of the Member State;***

(b) ***jeopardise an ongoing investigation of a criminal offence;***

(c) ***jeopardise the safety of an individual;***

(d) ***disclose information relating to organisations or specific intelligence activities in the field of national security;***

(e) ***disclose information which has initially been obtained from another Member State or a third country and that Member State or third country has, upon request, not given its consent to the provision of the information.***

Article 13

Use of SIENA

1. Member States shall ensure that, where their Single Point of Contact or their law enforcement authorities send requests for information, provide information pursuant to such requests, provide information on their own initiative [...] under Chapters II and III or under Article 12, they do so through SIENA.

1a. Member States may allow their SPOC or their law enforcement authorities not to use SIENA in the following cases:

(a) exchanges of information have been initiated through the Interpol communication channel;

(b) multilateral exchanges of information that also involve third countries or international organisations not connected to SIENA;

(c) exchanges of information can be faster with another communication channel for urgent requests;

(d) exchanges of information between Member States where unexpected technical or operational incidents suggest the use of another channel.

2. Member States shall ensure that their Single Point of Contact, as well as all their law enforcement authorities that may be involved in the exchange of information under this Directive, are directly connected to SIENA.

Chapter V

Single Point of Contact for information exchange between Member States

Article 14

Establishment, tasks and capabilities

1. Each Member State shall establish [...] one national Single Point of Contact, which shall be the central entity responsible for coordinating exchanges of information under this Directive.

2. Member States shall ensure that their Single Point of Contact is empowered to carry out at least all of the following tasks:

   (a) receive and evaluate requests for information ***submitted in accordance with Article 4***;

   (b) channel requests for information to the relevant national law enforcement [...] authorities and, where necessary, coordinate among them the processing of such requests and the provision of information upon such requests;

   (c) ***coordinate the*** analys[...]***is*** and ***the*** structur[...]***ing of*** information with a view to providing it to the [...] ***requesting*** Member States;

   (d) provide, upon request or upon [...] ***their*** own initiative, information to [...] other Member States in accordance with Articles 5 and 7;

(e) refuse to provide information in accordance with Article 6 and, where necessary, request clarifications in accordance with Article 6(3);

(f) send requests for information to the Single Points of Contact of other Member States in accordance with Article 4 and, where necessary, provide clarifications in accordance with Article 6(3).

3. Member States shall ensure that:

(a) their Single Point of Contact has access to all information available to their law enforcement authorities ***as defined in Article 2(4)***, insofar as necessary to carry out its tasks under this Directive;

(b) their Single Point of Contact carries out its tasks 24 hours a day, 7 days a week;

(c) their Single Point of Contact is provided with the staff, resources and capabilities, including for translation, necessary to carry out its tasks in an adequate and rapid manner in accordance with this Directive [...]***, including, where applicable***, the time limits set out in Article 5(1);

(d) the judicial authorities competent to grant the judicial authorisations required under national law in accordance with Article 9 are available ***on call*** to the Single Point of Contact 24 hours a day, 7 days a week.

4. Within one month of the establishment [...] of their Single Point of Contact, Member States shall notify the Commission thereof. They shall update that information where necessary.

The Commission shall publish those notifications, as well as any updates thereof, in the Official Journal of the European Union.

Article 15

Composition

1. Member States shall determine the organisation and the composition of [...] ***their*** Single Point of Contact in such a manner that it can carry out its tasks under this Directive in an efficient and effective manner.

2. Member States shall ensure that their Single Point of Contact is composed of representatives of national law enforcement authorities whose involvement is necessary for the adequate and rapid exchange of information under this Directive, including at least the following insofar as the Member State concerned is bound by the relevant legislation to establish or designate such units or bureaux:

   (a) the Europol national unit established by Article 7 of Regulation (EU) 2016/794;

   (b) the SIRENE Bureau established by Article 7(2) of Regulation (EU) 2018/1862 of the European Parliament and of the Council[34];

   (c) [...]

   (d) the INTERPOL National Central Bureau (NCB) established by Article 32 of Constitution of the International Criminal Police Organisation – INTERPOL.

[34] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312 7.12.2018, p. 56).

Article 16

Case Management System

1. Member States shall ensure that their Single Point of Contact deploys and operates an electronic single Case Management System as the repository that allows the Single Point of Contact to carry out its tasks under this Directive. The Case Management System shall have at least all of the following functions and capabilities:

   (a) recording incoming and outgoing requests for information referred to in Articles 5 and 8, as well as any other communications with Single Points of Contact and, where applicable, law enforcement authorities of other Member States relating to such requests, including the information about refusals and the requests for and provision of clarifications referred to in Article 6(2) and (3) respectively;

   (b) recording communications between the Single Point of Contact and national law enforcement authorities, pursuant to Article 15(2), point (b);

   (c) recording provisions of information to the Single Point of Contact and, where applicable, to the law enforcement authorities of other Member States in accordance with Articles 5, 7 and 8;

   (d) cross-checking incoming requests for information referred to in Articles 5 and 8, against information available to the Single Point of Contact, including information provided in accordance with the second subparagraph of Article 5(3) and the second subparagraph of Article 7(2) and other relevant information recorded in the Case Management System;

   (e) ensuring adequate and rapid follow-up to incoming requests for information referred to in Article 4, in particular with a view to respecting the time limits for the provision of the requested information set out in Article 5;

(f) be interoperable with SIENA, ensuring in particular that incoming communications through SIENA can be directly recorded in, and that outgoing communications through SIENA can be directly sent from, the Case Management System;

(g) generating statistics in respect of exchanges of information under this Directive for evaluation and monitoring purposes, in particular for the purpose of Article 17;

(h) logging of access and of other processing activities in relation to the information contained in the Case Management System, for accountability and cybersecurity purposes***, in accordance with Article 25 of Directive (EU) 2016/680***.

2. Member States shall take the necessary measures to ensure that all cybersecurity risks relating to the Case Management System, in particular as regards its architecture, governance and control, are managed and addressed in a prudent and effective manner and that adequate safeguards against unauthorised access and abuse are provided for.

3. Member States shall ensure that any personal data processed by their Single Point of Contact are contained in the Case Management System only for as long as is necessary and proportionate for the purposes for which the personal data are processed and are subsequently irrevocably deleted***, in accordance with Article 4(1)(e) and Article 5 of Directive (EU) 2016/680***.

Chapter VI

Final provisions

Article 17

Statistics

1. Member States shall provide the Commission with statistics ***of the previous year*** on the exchanges of information with other Member States under this Directive, by 1 March of each year.

2. The statistics shall cover, as a minimum:

   (a) the number of requests for information submitted by their Single Point of Contact and by their law enforcement authorities;

   (b) the number of requests for information received and replied to by the Single Point of Contact and by their law enforcement authorities, broken down by urgent and non-urgent, and broken down by the other Member States receiving the information;

   (c) the number of requests for information refused pursuant to Article 6, broken down per requesting Member States and per grounds of refusal;

   (d) the number of cases where the time limits referred to in Article 5(1) were deviated from due to having to obtain a judicial authorisation in accordance with Article 5(2), broken down by the Member States having submitted the requests for information concerned.

Article 18

Reporting

1. The Commission shall, by *[date of entry into force + 3 years]*, submit a report to the European Parliament and to the Council, assessing the implementation of this Directive.

2. The Commission shall, by *[date of entry into force + 5 years],* submit a report to the European Parliament and to the Council assessing the effectivity and effectiveness of this Directive. The Commission shall take into account the information provided by Member States and any other relevant information related to the transposition and implementation of this Directive. On the basis of this evaluation, the Commission shall decide on appropriate follow-up actions, including, if necessary, a legislative proposal.

Article 19

[...]

[...]

Article 20

Repeal

Framework Decision 2006/960/JHA is repealed from [the date referred to in Article 21(1), the first subparagraph].

References to that Framework Decision shall be construed as references to the corresponding provisions of this Directive.

Article 21

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by [*date of entry into force + 2 years*]. They shall forthwith communicate to the Commission the text of those provisions.

   They shall apply those provisions from that date. However, they shall apply Article 13 from [*date of entry into force + 4 years*].

   When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 22

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union.*

Article 23

Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*