Council of the European Union

Brussels, 9 December 2022
(OR. en)

15853/22

Interinstitutional File:
2021/0411(COD)

IXIM 296
ENFOPOL 632
JAI 1649
CODEC 1973
COMIX 611

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	15430/22
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 - Confirmation of the final compromise text with a view to agreement

At its meeting on 7 December 2022, the Permanent Representatives Committee agreed the final compromise text, as set out in the Annex to this note, with a view to reaching agreement with the European Parliament.

ANNEX

2021/0411 (COD)

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 ***pose a significant threat to the internal security of the Union and*** 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 ***increasingly dynamic and complex*** criminal activities***, which calls for an improved legal framework to ensure that competent law enforcement authorities can detect, prevent and investigate criminal offences in a more efficient manner***.

(2) ~~In an area without~~***For the development of the European area of freedom, security and justice, characterised by the absence of*** internal border controls, ~~police officers~~***it is essential that competent law enforcement authorities*** 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, ***competent*** 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~~***the purposes of preventing, detecting and investigating criminal offences***. Exchange of information on crime and criminal activities, including terrorism, serves the overall objective of protecting the security of natural persons ***and safeguarding important interests of legal persons protected by law***.

(2a) A majority of organised crime groups are present in more than three countries and are composed of members with multiple nationalities who engage in various criminal activities. The structure of such criminal groups is ever more sophisticated, with strong and efficient communication systems and cooperation between their members across borders.

(2b) To effectively fight cross-border crime, it is of paramount importance that competent law enforcement authorities swiftly exchange information and cooperate operationally with one another. Although cross-border cooperation between the competent law enforcement authorities of the Member States has improved in recent years, certain practical and legal hurdles continue to exist. In this respect, the Council Recommendation (EU) 2022/915 should assist the Member States in further enhancing the operational cross-border cooperation.

(2c) Some Member States have developed pilot projects to strengthen cross-border cooperation, focusing for example on joint patrols of police officers from neighbouring Member States in border regions. A number of Member States have also adopted bilateral or even multilateral agreements to strengthen cross-border cooperation, including information exchange. This Directive does not limit such possibilities, provided that the rules on information exchange are compatible with this Directive when it applies. On the contrary, Member States are encouraged to exchange best practice and lessons learnt from those pilot projects and agreements and to make use of available Union funding in that regard, in particular from the Internal Security Fund, established by Regulation (EU) 2021/1149 of the European Parliament and of the Council[1a]

(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[1], adopted on 19 June 1990, notably in its Articles 39 and 46. Council Framework Decision 2006/960/JHA[2] partially replaced those provisions and introduced new rules for the exchange of information and intelligence between Member States' ***competent*** law enforcement authorities.

(4) Evaluations, including those carried ***out*** under Council Regulation (EU) 1053/2013[3]~~,~~ 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.

---

1 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).

2 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).

3 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~~ ***should be updated with a view to eliminating discrepancies and establishing clear and harmonised rules*** 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 ***and to allow the competent law enforcement authorities to adapt to a rapidly changing and expanding organised crime landscape, inter alia in the context of the globalisation and digitalisation of society***.

(6) In particular, ~~the discrepancies between the relevant provisions of the Convention Implementing the Schengen Agreement and Framework Decision 2006/960/JHA~~***this Directive*** should ~~be addressed by covering~~***cover*** 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~~***the*** Convention ***Implementing the Schengen Agreement*** 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 ***harmonised*** rules governing the cross-cutting aspects of such information exchange between Member States ***at different stages of investigation, from the phase of gathering criminal intelligence to the phase of criminal investigation. 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 laid down in*** ~~. 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[4], (EU) 2018/1861[5], (EU) 2018/1862[6], and (EU) 2016/794[7] ***and (EU) .../... [[4a]] [on automated data exchange for police cooperation ("Prüm II")]*** of the European Parliament and of the Council, Directives (EU) 2016/681[8] and 2019/1153[9] of the European Parliament and of the Council, and Council Decisions 2008/615/JHA[10] and 2008/616/JHA[11].

---

4 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).

5 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).

6 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).

7 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).

8 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).

9 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).

10 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).

11 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.

(7a) A criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union. In the interest of effectively combating crime, the concept should be understood as referring to any conduct punishable under the criminal law of the Member State that is to receive the information, either pursuant to a request or pursuant to the own-initiative provision of information under this Directive, irrespective of the penalty that may be imposed in that Member State and irrespective whether the conduct is also punishable under the criminal law of the Member State providing the information, without prejudice however to the grounds for refusal set out in this Directive.

(7b) 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).

(7c) Since this Directive should not apply to the processing of information in the course of an activity which falls outside the scope of Union law, activities concerning national security should not be considered as 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) …/…[12] [on European Production and Preservation Orders for electronic evidence in criminal matters] and ***Directives 2014/41/EU***[1a] ***and*** Directive (EU) …/…[13] [laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings] ***of the European Parliament and of the Council***, unaffected. ***Consequently, whilst this Directive does not require so, Member States providing information under this Directive should be allowed to give their consent for the use of this 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.***

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

(9) All exchanges of information under this Directive should be subject to ~~three~~***five*** general principles, namely those of availability, equivalent access***, confidentiality, data ownership and data reliability*** ~~and confidentiality~~. ~~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~~***First***, the principle of availability should be understood as indicating that relevant information available to the Single Point of Contact or the ***competent*** 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~~. In addition~~***, as well as the obligation to have the consent of the State which initially provided the information to share it. Second***, 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. ***Third, the principle of confidentiality requires Member States to respect one another's national rules on confidentiality when treating information marked as confidential that is provided to the Single Point of Contact or to the competent law enforcement authority, by ensuring a similar level of confidentiality in accordance with the rules on confidentiality set out in national law. Fourth, pursuant to the principle of data ownership, information initially obtained from another Member State or third country should only be provided with the consent of and according to the conditions imposed by the country that initially provided the information. Fifth and finally, the principle of data reliability obliges that inaccurate, incomplete or obsolete data is erased, rectified or their processing restricted, as appropriate, and any recipient is notified without delay.***

(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.

(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 ***and in which language they are to be submitted***.

(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 ***competent*** 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 and any updates thereof, where relevant, should be provided by each Member State to the Commission, which should publish the lists online***. 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. ***Meanwhile, the Member States should seek to reduce the unjustified duplication of personal data to a strict minimum.***

(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 ~~a prior judicial authorisation is required~~***the information is directly or indirectly accessible by the Single Point of Contact or 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.***

(12a) The Single Points of Contact should assess whether the information requested is necessary for and proportionate to achieving the purposes of this Directive and whether the explanation of the objective reasons justifying the request is sufficiently clear and specific, so as to avoid unjustified provisions of information or the provision of disproportionate amounts of information.

(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 ***in full compliance with the rule of law***, those cases should be exhaustively specified 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. The Member States, as an expression of their general due diligence, should therefore always verify the compliance of incoming requests submitted to them under this Directive with the principles of necessity and proportionality and should refuse those requests they find to be non-compliant.*** 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~~***should*** be provided within the time limits set by this Directive. ~~Provision~~***In order to prevent unnecessary refusals, the Single Point of Contact or the designated law enforcement authority of the requesting Member State, as applicable,*** should ~~be made for the possibility to ask for clarifications~~***on request provide additional clarifications needed to process the request for information***, 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~~ ***by a Single Point of Contact or the competent law enforcement authorities to*** the Single Point of Contact or the ***competent*** law enforcement ~~authorities~~***authority of another Member State*** without a prior request***, namely the provision of information on their own initiative***. The second one is the provision of information upon requests for information submitted either by Single Points of Contact or by ***competent*** law enforcement authorities ~~not~~***directly*** to the ~~Single Point of Contact, but rather directly to the~~***competent*** 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 ***relevant*** 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. ***These requirements should apply also to situations where the competent law enforcement authority of a Member State provides such information to the Single Point of Contact of that Member State in order to provide such information to another Member State, such as in cases when compliance with language regime needs to be ensured.***

(15) The requirement of a prior judicial authorisation for the provision of information***, where provided in national law, constitutes*** ~~can be~~ an important safeguard ***which should be respected. However,*** ~~.~~ the Member States' legal systems are different in this respect and this Directive should not be understood as affecting ~~such requirements established under~~***the rules and conditions concerning prior judicial authorisation laid down in*** 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 ***competent*** 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 ***requesting*** Single Point of Contact or the ***designated*** law enforcement authority***, 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,*** ~~of another Member State that requested the information, to obtain the~~ judicial ~~authorisation as soon as possible~~***authorities may be concerned by 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~~ ***end, any personal data processing by a Single Point of Contact or a competent law enforcement authority under*** this Directive should be ~~aligned~~***carried out in full compliance*** with Directive (EU) 2016/680 of the European Parliament and of the Council[14]. ***The European Union Agency for Law Enforcement Cooperation (Europol) should process data in accordance with the rules set out in Regulation (EU) 2016/794 of the European Parliament and the Council[15]. That Directive and that Regulation remain unaffected by this Directive.*** In particular, it should be specified that any personal data exchanged by Single Points of Contacts and ***competent*** law enforcement authorities is to remain limited to the categories of data ***per category of data subject*** listed in Section B ~~point 2,~~ of Annex II to Regulation (EU) 2016/794***. Accordingly, a clear distinction should be made between the data concerning suspects and the data concerning witnesses, victims, or persons belonging to other groups, for which stricter limitations apply*** ~~of the European Parliament and of the Council~~. 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 Single Points of Contact or, where applicable, competent law enforcement authorities should process the requests for information pursuant to this Directive as quickly as possible to ensure the accuracy and reliability of the personal data, to avoid unnecessary duplication of*** ~~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***, and to reduce the risk of data becoming outdated or no longer being available to the requested competent law enforcement authority. If it appears that the personal data are incorrect, they should be rectified, erased or their processing restricted without delay*** ~~in connection to the activities under this Directive, should be carried out in compliance with the applicable~~

---

14 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).

15 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).

~~rules of Union law, in particular Directive (EU) 2016/680 and Regulation (EU) 2016/679 of the European Parliament and of the Council[16], which rules this Directive leaves unaffected~~.

(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~~***competent law enforcement authorities*** of the Member States concerned understand each other. ~~Language barriers often hamper the cross-border exchange of~~***To prevent delays in the provision of requested*** 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~~ ***caused by language barriers and to limit translation costs, Member States should establish a list of one or more languages in which their*** Single ~~Points~~***Point*** 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~~***can be addressed and in which it can communicate. All information exchanges, including the provision of the requested information, refusals, including the reasons for refusals, and, where applicable, requests for clarifications and the clarifications provided, related to a specific request should be transmitted in the language in which that request was submitted***. Therefore, Member States should establish a list containing one or more ~~official~~ languages of ~~the Union 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, which should publish online a compilation of such lists.***

---

16 ~~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).~~

(18) ***To ensure the safety and security of European citizens, it is essential that Europol holds the necessary information to fulfil its role***~~The further development of the European Union Agency for Law Enforcement Cooperation (Europol)~~ as the Union's criminal information hub ~~is a priority~~***supporting the competent law enforcement authorities***. That is why, when information ~~or any related communications are exchanged~~***is exchanged between Member States***, irrespective of whether that is done pursuant to a request for information submitted to a Single Point of Contact or ***competent*** law enforcement authority, or on their ~~own-imitative,~~ ***own-initative, an assessment should be made, on a case-by-case basis, as to whether*** a copy ***of the request made or information exchanged, pursuant to this Directive,*** should be sent to Europol~~, however only insofar as~~ ***where*** it concerns offences falling within the scope of the objectives of Europol ***and in line with Article 7(6) of Regulation (EU) 2016/794. Such assessment should be based on Article 3 of Regulation (EU) 2016/794, in so far as the scope of the criminal offences is concerned and Member States should not be obliged to copy Europol where one of the exceptions referred to in Article 7(7) of the same Regulation applies. Moreover, in accordance with the data ownership principle laid out in Article 3(4) of this Directive, it should be also considered that information initially obtained from another Member State or a third country should be provided to Europol only where that Member State or third country has given its consent. This provision is without prejudice to Article 19 of that Regulation pertaining to the determination of the purpose of, and restrictions on, the processing of information by Europol. Member States should ensure that their staff is adequately supported and trained to quickly and accurately identify which information exchanged in the context of this Directive falls within the mandate of Europol and is necessary for the Agency to fulfil its objectives***~~. In practice, this can be done through the ticking by default of the corresponding SIENA box~~.

(19) The proliferation of communication channels used for the transmission of law enforcement information between Member States ~~and of communications relating thereto~~ should be remedied, as it hinders the adequate and rapid exchange of such information ***and increases the risks concerning the security of personal data***. Therefore, the use of the secure information exchange network application ~~called~~ ***(‘***SIENA***’)***, managed ***and developed*** 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 ***competent*** 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~~***end***, all Single Points of Contact, as well as all ***competent*** law enforcement authorities that may be involved in such exchanges, should be directly connected to SIENA. ***To allow frontline officers, such as police officers involved in dragnet operations, to benefit from SIENA, it should also be operational on mobile devices, where appropriate.*** In this regard, a ***short*** transition period should be provided for, however, in order to allow for the full roll-out of SIENA***, as it entails a change of the current arrangements in some Member States and requires that staff to be trained.***
In order to take into account the operational reality and not to hamper good cooperation between competent law enforcement authorities, Member States should be able to allow their Single Points of Contact or their competent law enforcement authorities to use another secure communication channel in a limited number of justified situations. Where the urgency of the request leads to the use of another communication channel, the Member States concerned should, when practicable and consistent with operational needs, revert to using SIENA after the situation ceases to be urgent.

(20) In order to simplify, facilitate and better manage information flows, Member States should each establish or designate one Single Point of Contact competent for coordinating ***and facilitating*** information exchanges under this Directive. ***Each Member State, after establishing or designating its Single Point of Contact, should provide that information to the Commission for subsequent publication and should update that information where necessary.*** The Single Points of Contact should, in particular, contribute to mitigating the ***obstacles to information flows resulting from the*** fragmentation of the ***competent*** 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***, cybercrime, trafficking of human beings,*** 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~~***their*** own Member State, 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 ***in terms of budget and staff***, 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~~***could*** 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~~***staff of those competent*** 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 ***competent*** law enforcement authorities ~~competent~~***responsible*** for preventing, detecting or investigating criminal offences~~, as well as~~ ***and*** 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***, could be able to be represented in Single Points of Contact***. 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~~, the passenger information unit~~ and the Interpol National Central Bureau, as established under the relevant legislation ***or international agreement*** and notwithstanding this Directive not being applicable to information exchanges specifically regulated by such Union legislation.

(22a) Given the specific demands of cross-border law enforcement cooperation, including the handling of sensitive information in that context, it is essential for the staff of the Single Points of Contact and the competent law enforcement authorities to have the necessary knowledge and skills to carry out their functions under this Directive in a lawful, efficient and effective manner. In particular, the staff of the Single Point of Contact should be offered, and be encouraged to benefit from, adequate and regular training courses, provided both at Union and at national level, which correspond to their professional needs and specific backgrounds and which facilitate their contacts with Single Points of Contact and competent law enforcement authorities of other Member States needed for the application of the rules of this Directive. In this respect, particular attention should be paid to the proper use of data processing tools and IT systems, to imparting knowledge about the relevant Union and national legal frameworks in the area of Justice and Home Affairs, with a particular focus on protection of personal data, law enforcement cooperation and handling confidential information, and to the languages in which the Member State concerned has indicated that its Single Point of Contact is able to exchange information, with a view to helping overcome language barriers. For the purpose of providing the training, Member States should also, where appropriate, make use of the training courses and relevant tools offered by the European Union Agency for Law Enforcement Training (CEPOL), consider the possibility for the staff to spend a week at Europol, and make use of relevant offers made under programmes and projects funded by the Union budget, such as the CEPOL exchange programme.

(22b) In addition to technical skills and legal knowledge, mutual trust and common understanding are prerequisites for efficient and effective cross-border law enforcement cooperation under this Directive. Personal contacts acquired through joint operations and the sharing of expertise facilitate the building of trust and the development of a common Union culture of policing. They should also consider joint trainings and staff exchanges which focus on the transfer of knowledge about the working methods, investigative approaches and organisational structures of competent law enforcement authorities in other Member States.

(22c) To increase participation in training courses for the staff of the Single Points of Contact and the competent law enforcement authorities, Member States could also consider specific incentives for such staff.

(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 ***each of*** their tasks under this Directive in an effective and efficient manner, in particular as regards ***the exchange of*** information***. The Case*** Management ***System is a workflow system allowing Single Points of Contact to manage exchanges of information. The universal message format (UMF) standard established by Regulation (EU) 2019/818 should be encouraged to be used in the development of the Case Management System***.

(23a) The rules set out in Directive (EU) 2016/680 apply, in accordance with the requirements specified therein, to the processing including storage of personal data in the Case Management System. In the interest of clarity and effective protection of personal data, those rules should be further specified in this Directive. In particular, in accordance with Article 4(1)(e) of Directive (EU) 2016/680, it should be specified that, where a Single Point of Contact receives information exchanged under this Directive containing personal data, the Single Point of Contact should keep the personal data in the Case Management System only insofar as it is necessary and proportionate for it to carry out its tasks under this Directive. Where that is no longer the case, the Single Point of Contact should irrevocably delete the personal data from the Case Management System. In order to ensure that the personal data is kept only for as long as necessary and proportionate, in accordance with Article 5 of Directive (EU) 2016/680, the Single Point of Contact should regularly review whether those requirements continue to be met. For this purpose, the first review should take place at the latest 6 months after the exchange of information under this Directive has concluded, that is, the moment at which the last item of information has been provided or the latest communication relating thereto has been exchanged. The requirements of this Directive regarding such review and deletion should however not affect the possibility of the national authorities competent for the prevention, detection and investigation of criminal offences to keep the personal data in their national criminal files under national law, in compliance with Union law and in particular Directive (EU) 2016/680.

(23b) In order to assist Single Points of Contact and competent law enforcement authorities in carrying out the exchange of information under this Directive and to foster a common European police culture between Member States, the Member States should encourage their practical cooperation. In particular, the Council should organise meetings of the Heads of the Single Points of Contact at least on an annual basis to exchange experience and best practice regarding information exchanges for the purposes of this Directive. Other forms of cooperation should include the drafting of manuals on law enforcement information exchange, compilation of national fact sheets containing information on directly and indirectly accessible information, Single Points of Contact, designated law enforcement authorities and language regimes, or other documents on common procedures, the addressing of difficulties regarding workflows, awareness-raising about specificities of relevant legal frameworks and organising, as appropriate, meetings between relevant Single Points of Contact.

(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 ***concerning the implementation of this Directive***. This requirement is necessary, in particular, to remedy the lack of comparable data quantifying relevant ***cross-border*** information exchanges ***between competent law enforcement authorities*** and also facilitates the reporting obligation of the Commission ***regarding the implementation of this Directive. 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~~***prevent, detect or investigate*** such criminal offences. Adequate and rapid information flows between relevant ***competent*** 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 ***and a common culture*** on the exchange of information ***and through modern tools and communication channels***. 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.

(25a) The European Data Protection Supervisor was consulted in accordance with Article 41(2) of Regulation (EU) 2018/1725 of the European Parliament and the Council, and delivered an opinion on 7 March 2022.

(25b) This Directive builds upon the values on which the Union is based, as set out in Article 2 of the Treaty on European Union, including the rule of law, freedom and democracy. It also respects fundamental rights and safeguards and observes the principles recognised by the Charter of Fundamental Rights of the European Union (the 'Charter'), in particular the right to liberty and security of a person, the respect for private and family life and the right to the protection of personal data as provided for by Articles 6, 7, and 8 of the Charter, as well as by Article 16 of the Treaty on the Functioning of the European Union (TFEU). Any processing of personal data under this Directive should be limited to that which is strictly necessary and proportionate and subject to clear conditions, strict requirements and effective supervision by the national supervisory authorities and the European Data Protection Supervisor, where appropriate in accordance with their respective mandates.

(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[17]; Ireland is therefore taking part in the adoption of this Directive and is bound by it.

[17] 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).

(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[18] which fall within the area referred to in Article 1, point H of Council Decision 1999/437/EC[19].

(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[20] 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[21] and with Article 3 of Council Decision 2008/149/JHA[22].

---

18 OJ L 176, 10.7.1999, p. 36.

19 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).

20 OJ L 53, 27.2.2008, p. 52.

21 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).

22 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[23] 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[24] and with Article 3 of Council Decision 2011/349/EU[25],

HAVE ADOPTED THIS DIRECTIVE:

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

[24] 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).

[25] 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 ***harmonised*** rules for the ***adequate and rapid*** exchange of information between the ***competent*** law enforcement authorities of the Member States ~~where necessary~~ for the purpose 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 or designated by the Member States, in particular on the content of such requests, ~~mandatory time limits for providing the requested information, reasons for refusals of such requests and the channel of communication to be used in connection to~~***the provision of information pursuant to such requests, the working languages of the Single Points of Contact, 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 ***competent*** law enforcement authorities of other Member States, in particular the situations and the manner in which such information is to be provided;

(c) the ***default*** channel of communication to be used for all exchanges of information ***pursuant to this Directive*** and the information to be provided to the Single Points of Contact in relation to exchanges of information directly between the ***competent*** law enforcement authorities of the Member States;

(d) the establishment ***or designation, organisation***, tasks, composition and capabilities of ~~the~~***each Member State's*** Single Point of Contact, including on the deployment ***and operation*** of a single electronic Case Management System for the fulfilment of ~~its~~***their*** tasks~~.~~ ***under this Directive;***

2. This Directive shall not apply to exchanges of information between the ***competent*** 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.***

3. This Directive does not impose any obligation on Member States to:

(a) obtain information by means of coercive measures~~, taken in accordance with national law, for the purpose of providing it to the law enforcement authorities of other Member States~~;

(b) store ***any*** information for the ***sole*** purpose ~~referred to in point (a)~~***of providing it to the competent law enforcement authorities of other Member States***;

(c) provide information to the ***competent*** 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.***

Article 2

Definitions

For the purpose of this Directive:

(1) '***competent*** law enforcement authority' means any ***police, customs or other*** authority of the Member States competent under national law ***to exercise authority and to take coercive measures*** for the purpose of preventing, detecting or investigating criminal offences***, and any authority that takes part in joint entities set up between two or more Member States 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 Article 47 of the Convention Implementing the Schengen Agreement are not covered by this definition***;

(1a) 'designated law enforcement authority' means a competent 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[26];

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

(c) ~~tax crimes relating to direct and indirect taxes, as laid down in national law;~~

(3) 'information' means any content concerning one or more natural ***or legal*** persons, facts or circumstances relevant to ***competent*** law enforcement authorities ~~in connection to the exercise of~~ ***for the purpose of exercising*** their tasks under national law of preventing, detecting or investigating criminal offences***, including criminal intelligence***;

[26] 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).

(4) '***information*** available' ~~information~~ means information that is ~~either held~~***directly or indirectly accessible*** by the Single Point of Contact or the law enforcement authorities of the requested Member State~~, 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 without coercive measures~~;

(4a) 'directly accessible information' means information that is held in a database that can be directly accessed by the Single Point of Contact or the law enforcement authorities of the requested Member State;

(4b) 'indirectly accessible information' means information that Single Points of Contact or 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.

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

(6) 'personal data' means personal data as defined in Article ~~4~~***3***, point (1)***, of Directive (EU) 2016/680*** ~~of Regulation (EU) 2016/679~~.

Article 3

Principles of information exchange

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

(a) ~~any relevant information~~ available ~~to the Single Point of Contact or the law enforcement authorities of Member States is~~***information can be*** provided to the Single Point of Contact or the law enforcement authorities of other Member States ('principle of availability');

(b) the conditions for requesting information from ~~the Single Point of Contact or the law enforcement authorities of other Member States, and those for~~***and*** providing information to the Single Points of Contact and the ***competent*** law enforcement authorities of other Member States, are equivalent to those applicable for requesting and providing similar information ~~from and to their own law enforcement authorities~~***within the Member States involved*** (‘principle of equivalent access’);

(c) information provided to the Single ~~Point~~***Points*** of Contact or the ***competent*** law enforcement authorities of ~~another~~***other*** Member ~~State~~***States*** that is marked as confidential is protected by ~~those law enforcement authorities~~***them*** 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').

(e) personal data exchanged under this Directive that is found to be inaccurate, incomplete or no longer up to date is erased, rectified or their processing restricted, as appropriate, and any recipient is notified without delay ('principle of data reliability')

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, their~~***their national law so provides, the designated*** law enforcement authorities**,** submit ~~requests for information~~ to the Single ~~Points~~***Point*** of Contact of ~~other~~***another*** Member ~~States in accordance~~***State complies*** with the conditions set out in paragraphs 2 to 5.

Member States shall notify the Commission with the list of their designated law enforcement authorities. They shall update that information where necessary.

~~Where a~~ Member ~~State has decided that, in addition to its Single Point of Contact, its law enforcement authorities may also submit requests for information~~***States shall ensure that theirdesignated law enforcement authorities send, at the same time as submitting such requests, a copy of those requests*** to the Single ~~Points~~***Point*** of Contact of ~~other Member States, it shall ensure that those authorities send, at the same time as submitting such requests, a copy of those requests, and of any other communication relating thereto, to the Single Point of Contact of that Member State~~***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, on a case by case basis, 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 where that would jeopardise:***

(a) ***an ongoing highly sensitive investigation which needs an appropriate level of confidentiality for the processing of their information;***

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

(c) ***the safety of an individual.***

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); ***and***

(b) the requested information is available to ~~the law enforcement authorities of the requested~~***that*** Member State.

3. Any request for information to the Single Point of Contact of another Member State shall specify ***and justify*** 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 a person's vital interests which are at imminent risk~~***prevent an imminent threat to life or the physical integrity of a person***;

(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 ***and the information is considered important for the prevention, detection or investigation of criminal offences***.

4. Requests for information to the Single Point of Contact of another Member State shall contain all necessary ~~explanations~~***details*** 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 the ~~law enforcement authorities of the~~ requested Member State;

(d) an explanation of the connection between the purpose and ~~the~~***any natural or legal*** person***, or subject, to which*** ~~or persons to whom~~ the information relates, where applicable;

(e) the reasons for which the request is considered urgent, where applicable~~.~~***, in accordance with paragraph 3;***

(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 ~~in any event~~ within the following time limits, as applicable:

   (a) eight hours, for urgent requests relating to information that is ~~available to the law enforcement authorities of~~***directly accessible by*** the requested Member State***;*** ~~without having to obtain a judicial authorisation;~~

   (b) three calendar days, for urgent requests relating to information that is ~~available to the law enforcement authorities of~~***indirectly accessible by*** the requested Member State ~~subject to a requirement to obtain a judicial authorisation~~***;***

   (c) seven calendar days, for all ~~requests that are not urgent~~***other requests***.

   The time ~~periods~~***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 ~~referred to~~***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 Single Point of Contact or, where applicable, the ***designated*** law enforcement authority of 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 Single Point of Contact or, where applicable, the ***designated*** law enforcement authority of 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.

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.

Article 6

Refusals of requests for information

1. 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) the requested information is not available to the Single Point of Contact and ~~the~~ ***the competent*** law enforcement authorities of the requested Member State;

(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) the requested information constitutes personal data other than that falling within the categories of personal data referred to in Article 10, point (i);

(da) the requested information has been found to be inaccurate, incomplete or no longer up to date and cannot be provided in accordance with Article 7(2) of Directive (EU) 2016/680;

(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 the success of an ongoing investigation of a criminal offence~~;~~ or ***the safety of an individual***;

(iii) unduly harm the ~~vital~~***protected important*** interests of a ~~natural or~~ legal person.

(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 not given its consent to the provision of the information.

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 of Article 4(1), in particular as to whether there is a manifest breach of fundamental rights.

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 Single Point of Contact or, where applicable, the ***designated*** law enforcement authority of the requesting Member State of the refusal, specifying the reasons for the refusal, within the time limits provided for in Article 5(1).

3. ***Where relevant, requested*** Member States shall ensure that their Single Point of Contact immediately requests ~~additional clarifications needed to process a request for information that otherwise would have to be refused~~**,** from the Single Point of Contact or, where applicable, the ***designated*** law enforcement authority of the requesting Member State**,** ***additional clarifications or sufficient specifications 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 Single Point of Contact or, where applicable, the ***designated*** law enforcement authority of the requesting Member State receives the request for clarifications ***or specifications***, until the moment ~~that the Single Point of Contact of~~ the requested ~~Member State receives the clarifications~~***clarifications or specifications are provided***.

4. The refusals, reasons for the refusals, requests for clarifications ***or specifications*** and clarifications ***or specifications*** referred to in ~~paragraphs 3 and 4~~***paragraph 3***, 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 competent law enforcement authorities, information available to them to the Single Points of Contact or to the competent 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 ***competent*** law enforcement authorities provide, on their own initiative, ~~any~~ information available to them to the Single Points of Contact or to the ***competent*** 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 referred to~~***purposes of preventing, detecting or investigating serious criminal offences as defined*** in Article ~~1(1)~~***2(2)***. However, no such obligation shall exist insofar as the reasons referred to in points (c),~~(d)~~ 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 ***competent*** 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 requested~~***that other*** Member State and published in accordance with Article 11.

Member States shall ensure that, where their Single Point of Contact ~~or their~~***provides such information to the*** law enforcement ~~authorities provide such~~***authority of another Member State, it also sends, 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 competent*** law enforcement ~~authority of~~***authorities provide such information to*** another Member State, they also send, at the same time, a copy of that information ***to their own Single Point of Contact and, where appropriate,*** 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 competent law enforcement authorities not to send, at the same time as providing information to the Single Point of Contact or the competent 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~~***Point*** of Contact ~~or law enforcement authorities~~ submit requests for information directly to the ***competent*** law enforcement authorities of another Member State, ~~their Single Points of Contact or their law enforcement authorities send~~***it provides***, at the same time***, a copy of those*** ~~as they send such~~ requests~~, provide information pursuant to such requests or send any~~ ***to the Single Point of Contact of that*** other ~~communications relating thereto, a copy thereof to the Single Point of Contact of that other Member State and, where the sender is a law enforcement authority, also to the~~***Member State. Member States shall ensure that, where their competent 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 ~~of its own Member State~~.

2. Member States shall ensure that, where their competent law enforcement authorities submit requests for information or provide information pursuant to such requests directly to the competent law enforcement authorities of another Member State, they provide, at the same time, a copy of that request or that information to their 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 Single Point of Contact or competent law enforcement authorities not to send the copies referred to in paragraph 1 or 2.

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 competent*** law enforcement authority of another Member State under Chapters II and III, where no such requirement applies ~~in respect of~~***for providing*** similar ~~provision of~~ information ~~to their own Single Point of Contact or their own law enforcement authorities~~***within the Member State involved***.

2. Member States shall ensure that, where their national law requires a judicial authorisation for the provision of information to ~~the Single Points of Contact or the law enforcement authority of~~ another Member State in accordance with paragraph 1, their Single ~~Points~~***Point*** of Contact or their ***competent*** 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~~***2*** 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 ***competent*** law enforcement authorities provide information under Chapters II and III that constitutes personal data:

-i ***the personal data are accurate, complete and up to date, in accordance with the requirements of Article 7(2) of the Directive (EU) 2016/680;***

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

(ii) their Single Point of Contact or their ***competent*** law enforcement authorities also provide, at the same time and ~~insofar~~***in so far*** as possible, the necessary elements enabling the Single Point of Contact or the ***competent*** 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~~ official~~ languages~~ of the Union~~ in which their Single Point of Contact is able to ~~provide information upon a request for~~***exchange*** information~~ or on its own initiative~~. That list shall include English.

2. Member States shall provide those lists, as well as any updates thereof, to the Commission. The Commission shall publish ~~those~~***online a compilation of such national*** lists~~,~~ as well as any updates thereof~~, in the Official Journal of the European Union~~.

Article 12

Provision of information to Europol

1. Member States shall ensure that, where their Single Point of Contact or their ***competent*** law enforcement authorities send requests for information, provide information pursuant to such requests, provide information on their own initiative ~~or send other communications relating thereto~~ under Chapters II and III, ~~they also send, at the same time,~~ ***their staff also assess, on a case-by-case basis and in accordance with Article 7(7) of Regulation (EU) 2016/794, whether it is necessary to send*** a copy thereof to Europol, ~~insofar~~***in so far*** as the information to which the communication relates concerns offences falling within the scope of the objectives of Europol in accordance with ***Article 3 of*** Regulation (EU) 2016/794.

2. ***Member States shall ensure that the purposes of the processing and any possible restrictions pursuant to Article 19 of Regulation (EU) 2016/794 are duly communicated to Europol when information is transmitted pursuant to paragraph 1 and that information initially obtained from another Member State or a third country is provided only where that Member State or third country has given its consent.***

Article 13

~~Use of SIENA~~***Secure communication channel***

1. Member States shall ensure that, where their Single Point of Contact or their ***competent*** law enforcement authorities send requests for information, provide information pursuant to such requests, provide information on their own initiative~~ or send other communications relating thereto~~ under Chapters II and III or under Article 12, they do so through ***the Secure Information Exchange Network Application of Europol (***SIENA***)***.

1a. Member States may allow their Single Point of Contact or their competent law enforcement authorities not to use SIENA in the following cases:

(a) exchanges of information that also require the involvement of third countries or international organisations or, for which there are objective reasons to believe that such involvement will be required at a later stage, including through the Interpol communication channel;

(b) the urgency of the request requires the temporary use of another communication channel;

(c) exchanges of information between Member States where unexpected technical or operational incidents prevent its use.

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

Chapter V

Single Point of Contact for information exchange between Member States

Article 14

Establishment ***or designation***, tasks and capabilities

1. Each Member State shall establish or designate one national Single Point of Contact, which shall be the central entity responsible for coordinating ***and facilitating*** exchanges of information under this Directive.

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

   (a) receive and evaluate requests for information ***submitted in accordance with Article 4 in the languages notified pursuant to Article 11(2)***;

   (b) channel requests for information to the ~~appropriate~~***relevant competent*** national law enforcement ~~authority or~~ authorities and, where necessary, coordinate among them the processing of such requests and the provision of information upon such requests;

   (c) ~~analyse and structure~~***coordinate the analysis and the structuring of*** information with a view to providing it to the Single Points of Contact and, where applicable, to the ***competent*** law enforcement authorities of other Member States;

   (d) provide, upon request or upon its own initiative, information to ~~the Single Points of Contact and, where applicable, to the law enforcement authorities of~~ 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 ***or specifications*** 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 ***or specifications*** 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 ***competent*** law enforcement authorities, 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~~***qualified*** staff, ***appropriate operational tools, technical and financial*** resources***, infrastructure,*** and capabilities, including for translation, necessary to carry out its tasks in an adequate***,*** ***effective*** and rapid manner in accordance with this Directive***, including, where applicable,*** ~~and in particular~~ 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 or designation 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

Organisation, composition ***and training***

1. Member States shall determine the organisation and the composition of ~~its~~***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~~***staff of their competent*** law enforcement authorities whose involvement is necessary for the adequate and rapid exchange of information under this Directive, including at least the following ~~insofar~~***in so far*** as the Member State concerned is bound by the relevant legislation ***or international agreement*** 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[27];

   (c) ~~the passenger information unit established under Article 4 of Directive (EU) 2016/681;~~

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

[27] 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).

2a. Member States shall ensure that the staff of their Single Points of Contact are adequately qualified for their tasks in order to enable them to perform their functions under this Directive. To that end, Member States shall provide the staff with access to adequate and regular training, in particular as regards the following:

(a) the use of data processing tools used within the Single Point of Contact, in particular SIENA and the Case Management System;

(b) the application of Union and national law relevant for the activities of the Single Point of Contact under this Directive, in particular on the protection of personal data, including Directive (EU) 2016/680, on cross-border cooperation between law enforcement authorities, including this Directive and Regulation (EU) 2016/794, and on the handling of confidential information;

(c) the use of the languages included in the list established by the Member State concerned pursuant to Article 11.

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, ***competent*** law enforcement authorities of other Member States relating to such requests, including the information about refusals and the requests for and provision of clarifications ***or specifications*** referred to in Article 6(2) and (3) respectively;

(b) recording communications between the Single Point of Contact and ~~national~~***the competent*** 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 ***competent*** 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 ***the Case Management System contains*** 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~~***only for as long as it is necessary and proportionate for the Single Point of Contact to carry out the tasks assigned to it under this Directive and that*** the personal data ~~are processed and~~***contained therein*** are subsequently irrevocably deleted.

3a. Member States shall ensure that their Single Point of Contact reviews, for the first time at the latest six months after the exchange of information has concluded and subsequently on a regular basis, compliance with paragraph 3.

Article 16a

Cooperation between Single Points of Contact

1. Member States shall encourage the practical cooperation between their Single Point of Contact and competent law enforcement authorities for the purposes of this Directive.

2. Member States shall ensure that the Heads of the Single Points of Contact meet at least once a year to assess the quality of the cooperation between their services, to discuss necessary technical or organisational measures in the event of any difficulties and to clarify procedures where required.

Chapter VI

Final provisions

Article 17

Statistics

1. ***By 1 March of each year,*** Member States shall provide the Commission with statistics on the exchanges of information with other Member States under this Directive~~, by 1 March of each~~ ***which took place during the previous calendar*** year.

2. The statistics shall cover, as a minimum:

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

   (b) the number of requests for information received and replied to by the Single Point of Contact and by their ***competent*** 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~~***for*** 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.

2a. The Commission shall compile the minimum statistics provided by Member States in accordance with paragraph 2, (a) to (d), and make them available to the European Parliament and to the Council.

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 ***and containing detailed information on how each Member State has implemented it. In compiling that report, the Commission shall pay particular attention to the efficiency of the exchange of information between competent authorities, the grounds for which requests for information were refused, in particular where the request falls outside the scope of the objectives of this Directive, and the compliance with provisions on data protection and the transferring of information to Europol***.

2. The Commission shall, by [date of entry into force + ~~5~~***4*** years], submit a report to the European Parliament and to the Council assessing the ~~effectivity and effectiveness of this Directive~~***effectiveness of this Directive, in particular its impact on law enforcement cooperation, the obligations laid down in Article 14(3), point (c), and the protection of personal data***. 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***, including, where applicable, practical obstacles that hamper its effective implementation***. On the basis of this evaluation, the Commission shall decide on appropriate follow-up actions, including, if ~~necessary~~***appropriate***, a legislative proposal.

2a. The Commission shall submit the reports referred to in paragraphs 1 and 2 every five years after the date referred to in paragraph 2.

Article 19

Amendments to the Convention Implementing the Schengen Agreement

From [the date referred to in Article 21(1), the first subparagraph], the Convention Implementing the Schengen Agreement***, for those parts that were not already replaced by Framework Decision 2006/960/JHA,***
-is amended as follows:

~~(i)~~ ~~Article 39 is~~***Articles 39 and 46 are*** replaced by this Directive insofar as ~~that article relates~~***these articles relate*** to the exchange of information ~~for the purpose referred to in Article 1(1)~~***within the scope*** of this Directive~~;~~**.**

~~(ii)~~ ~~Article 46 is deleted.~~

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~~***18 months***]. 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*