I

(Legislative acts)

DIRECTIVES

DIRECTIVE (EU) 2023/977 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 10 May 2023

on the exchange of information between the law enforcement authorities of Member States and 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 [1],

Whereas:

(1) Transnational 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 crime and terrorism, action at Union level is paramount to ensuring efficient and effective cooperation as regards the exchange of information. Furthermore, organised crime and terrorism, in particular, are emblematic of the link between internal and external security. Transnational criminal activities 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. There is, therefore, a need for an improved legal framework to ensure that competent law enforcement authorities can prevent, detect and investigate criminal offences in a more efficient manner.

(2) For the development of an area of freedom, security and justice, which is characterised by the absence of internal border controls, it is essential that competent law enforcement authorities in one Member State 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 that regard, competent law enforcement authorities should cooperate effectively and across the Union. Therefore, police cooperation on the exchange of relevant information for the purpose of preventing, detecting or investigating criminal offences is an essential component of the measures that underpin public security in an interdependent area without internal border controls. The 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.

[1] Position of the European Parliament of 15 March 2023 (not yet published in the Official Journal) and decision of the Council of 24 April 2023.

(3) The 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 organised crime groups is ever more sophisticated, with strong and efficient communication systems and cooperation between their members across borders.

(4) To fight cross-border crime effectively, 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 has improved in recent years, certain practical and legal hurdles continue to exist. In that respect, Council Recommendation (EU) 2022/915 ([2]) will assist the Member States in further enhancing cross-border operational cooperation.

(5) Some Member States have developed pilot projects to strengthen cross-border cooperation, focusing, for example, on joint patrols by police officers from neighbouring Member States in border regions. A number of Member States have also concluded bilateral or even multilateral agreements to strengthen cross-border cooperation, including the exchange of information. This Directive does not limit such possibilities, provided that the rules on the exchange of information set out in such agreements are compatible with this Directive where it applies. On the contrary, Member States are encouraged to exchange best practice and lessons learnt from such 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 ([3]).

(6) The exchange of information between Member States for the purpose of preventing and detecting criminal offences is regulated by the Convention implementing the Schengen Agreement of 14 June 1985 ([4]), adopted on 19 June 1990, in particular Articles 39 and 46 thereof. Council Framework Decision 2006/960/JHA ([5]) partially replaced those provisions and introduced new rules for the exchange of information and intelligence between competent law enforcement authorities.

(7) Evaluations, including those carried out under Council Regulation (EU) No 1053/2013 ([6]), have indicated that Framework Decision 2006/960/JHA is not sufficiently clear and does not ensure the adequate and rapid exchange of relevant information between Member States. Evaluations have also indicated that that Framework Decision is scarcely used in practice, in part due to the lack of clarity encountered in practice between the scope of the Convention implementing the Schengen Agreement and the scope of that Framework Decision.

(8) Therefore, the existing legal framework should be updated with a view to eliminating discrepancies and to establishing clear and harmonised rules to facilitate and ensure 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 the rapidly changing and expanding nature of organised crime, including in the context of the globalisation and digitalisation of society.

([2]) Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation (OJ L 158, 13.6.2022, p. 53).

([3]) Regulation (EU) 2021/1149 of the European Parliament and of the Council of 7 July 2021 establishing the Internal Security Fund (OJ L 251, 15.7.2021, p. 94).

([4]) 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).

([5]) 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).

([6]) 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).

(9) In particular, this Directive should cover the exchange of information for the purpose of preventing, detecting or investigating criminal offences, thereby fully superseding, in so far as such exchanges are concerned, Articles 39 and 46 of the Convention implementing the Schengen Agreement and providing the necessary legal certainty. In addition, the relevant rules should be simplified and clarified in order to facilitate their effective application in practice.

(10) It is necessary to lay down harmonised rules governing the crosscutting aspects of the exchange of information between Member States under this Directive at different stages of an investigation, from the phase of gathering criminal intelligence to the phase of criminal investigation. Those rules 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. However, those rules should not include the bilateral exchange of information with third countries. The rules laid down in this Directive should not affect the application of rules of Union law on specific systems or frameworks for such exchanges, such as Regulations (EU) 2016/794 ([7]), (EU) 2018/1860 ([8]), (EU) 2018/1861 ([9]) and (EU) 2018/1862 ([10]) of the European Parliament and of the Council, Directives (EU) 2016/681 ([11]) and (EU) 2019/1153 ([12]) of the European Parliament and of the Council, and Council Decisions 2008/615/JHA ([13]) and 2008/616/JHA ([14]).

(11) 'Criminal offence' is an autonomous concept of Union law as interpreted by the Court of Justice of the European Union. For the purposes of this Directive, in the interest of effectively combating crime, 'criminal offence' should be understood as referring to any conduct punishable under the criminal law of the Member State that receives information, either pursuant to a request or pursuant to an own-initiative provision of information in accordance with this Directive, irrespective of the penalty that can be imposed in that Member State and irrespective of whether the conduct is also punishable under the criminal law of the Member State that provides information, without prejudice to the grounds for refusal of requests for information set out in this Directive.

(12) This Directive is without prejudice to 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 ([15]) (Naples II).

(13) Since this Directive does 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 do not fall within the scope of this Directive.

([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]) 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).

([9]) 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 (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14).

([10]) 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).

([11]) 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).

([12]) 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).

([13]) 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).

([14]) 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).

([15]) OJ C 24, 23.1.1998, p. 2.

(14) 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 in accordance with this Directive as evidence and, consequently, it does not affect any requirement provided for in the applicable law to obtain the consent of the Member State providing the information for such use. This Directive does not affect Union legal acts on evidence, such as a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, Directive 2014/41/EU of the European Parliament and of the Council ([16]) and a Directive of the European Parliament and of the Council laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. Consequently, even though they are not required to do so under this Directive, Member States providing information under this Directive should be allowed to consent, at the time of providing the information or thereafter, to the use of that information as evidence in judicial proceedings, including, where necessary under national law, through the use of instruments regarding judicial cooperation in force between the Member States.

(15) All exchanges of information under this Directive should be subject to five general principles, namely the principles of availability, equivalent access, confidentiality, data ownership and data reliability. While those principles are without prejudice to the more specific provisions of this Directive, they should guide its interpretation and application where relevant. 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 the Single Point of Contact or the competent law enforcement authorities of other Member States. However, that 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 on judicial authorisations, or of the obligation to obtain the consent of the Member State or third country that initially provided the information prior to sharing it. Second, pursuant to the principle of equivalent access, Member States should ensure that the access that the Single Point of Contact and the competent law enforcement authorities of other Member States have to relevant information is substantially the same as, and thus neither stricter nor less strict than, the access that their own Single Point of Contact and the competent law enforcement authorities have to that information, subject to the more specific provisions of this Directive. 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 their Single Point of Contact or to their competent law enforcement authorities, 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 from a third country should only be provided with the consent of and in accordance with the conditions imposed by that Member State or third country. Fifth, pursuant to the principle of data reliability, personal data that are found to be inaccurate, incomplete or no longer up to date should be erased or rectified or the processing of those data should be restricted, as appropriate, and any recipient of those data should be notified without delay.

(16) In order to achieve the objective of facilitating and ensuring the adequate and rapid exchange of information between Member States, this Directive should provide the possibility for Member States to obtain information by addressing a request for information to the Single Point of Contact of other Member States, in accordance with certain clear, simplified and harmonised requirements. As regards the content of requests for information, this Directive should specify, in particular, in an exhaustive and sufficiently detailed manner and without prejudice to the need for a case-by-case assessment, the situations in which requests for information are to be considered urgent, the details they are to contain as a minimum and in which language they are to be submitted.

(17) While the Single Points of Contact of each Member State should, in any event, be able 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, in addition, to designate some of their competent law enforcement authorities, which might be involved in European cooperation, as designated law enforcement authorities for the purpose of submitting such requests to the Single Points of Contact of other Member States. Each Member State should submit to the Commission a list of its designated law enforcement authorities. Member States should inform the Commission

([16]) Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014, p. 1).

where there are any changes to that list. The Commission 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 decides to allow some of its competent law enforcement authorities to submit requests for information to the Single Points of Contact of other Member States, that Member State makes its Single Point of Contact aware of all outgoing requests for information and of any communications relating thereto, by always putting its Single Point of Contact in copy. Member States should seek to limit the unjustified duplication of personal data to a strict minimum.

(18) Time limits are necessary to ensure the rapid processing of requests for information submitted to a Single Point of Contact. Time limits should be clear and proportionate and take into account whether the request for information is to be considered as urgent and whether the request relates to directly accessible information or indirectly accessible information. In order to ensure compliance with the applicable time limits while allowing for a degree of flexibility, where objectively justified, it should only be possible, on an exceptional basis, to deviate from those time limits where, and in so 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 ensure, as far as possible, that time-critical opportunities to take action in specific cases are not missed, the requested Member State should provide any requested information as soon as it is held by the Single Point of Contact, even where that information is not the only information available that is relevant to the request. The rest of the requested information should be provided thereafter, as soon as it is held by the Single Point of Contact.

(19) 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 detailed, so as to avoid the unjustified provision of information or the provision of disproportionate amounts of information.

(20) In exceptional cases, it might be objectively justified for a Member State to refuse a request for information submitted to its 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 specified exhaustively and interpreted restrictively. However, the rules set out in this Directive place a strong emphasis on the principles of necessity and proportionality, thereby providing safeguards against any misuse of requests for information, including where it would entail manifest breaches of fundamental rights. The Member States, as an expression of their general due diligence, should therefore always verify the compliance of 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. Where the reasons for refusing the request relate only to parts of the information requested, the remaining information should be provided within the time limits set out in this Directive. In order to prevent unnecessary refusals of requests for information, the Single Point of Contact or the designated law enforcement authority of the requesting Member State, as applicable, should, on request, provide clarification or specifications that are needed to process the request for information. The applicable time limits should 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 clarification or specifications. However, it should be possible to request clarification or specifications only where clarification or specifications are objectively necessary and proportionate such that without them the request for information would have to be refused for one of the reasons listed in this Directive. In the interest of effective cooperation, it should also remain possible to request necessary clarification or specifications in other situations, without this leading to the suspension of the time limits.

(21) In order to allow for the necessary flexibility in view of operational needs that might vary in practice, this Directive should provide for two other means of exchanging information, in addition to requests for information submitted to the Single Points of Contact. The first one is the unsolicited provision of information by a Single Point of Contact or by a competent law enforcement authority to the Single Point of Contact or a competent law enforcement authority of another Member State without a prior request, namely the provision of information on its own initiative. The second one is the provision of information upon a request for information submitted either by a Single Point of Contact or by a competent law enforcement authority directly to a competent law enforcement authority of another Member State. In respect of both means of exchange of information, this Directive sets out only a limited number of minimum requirements, in particular on keeping the relevant Single Points of Contact

informed and, as regards own-initiative provisions of information, the situations in which information is to be provided and the language to be used. Those requirements should also apply to situations in which a competent law enforcement authority provides information to the Single Point of Contact of its own Member State in order to provide that information to another Member State, such as where it is necessary to comply with the rules set out in this Directive on the language to be used when providing information.

(22) The requirement of a prior judicial authorisation for the provision of information, where provided in national law, constitutes an important safeguard which should be respected. However, the Member States' legal systems are different in that respect and this Directive should not be understood as affecting the rules and conditions concerning prior judicial authorisations laid down in national law, other than requiring that domestic exchanges and exchanges between Member States be treated in an equivalent manner, both on 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 Single Point of Contact or the designated law enforcement authority of the requesting Member State, to obtain the judicial authorisation as soon as possible. Although the legal basis of this Directive is limited to law enforcement cooperation under Article 87(2), point (a), of the Treaty on the Functioning of the European Union (TFEU), this Directive might be of relevance to judicial authorities.

(23) It is particularly important that the protection of personal data, in accordance with Union law, be ensured in connection with all exchanges of information under this Directive. To that end, any personal data processing by a Single Point of Contact or a competent law enforcement authority under this Directive should be carried out in full compliance with Directive (EU) 2016/680 of the European Parliament and of the Council ([17]). Pursuant to Regulation (EU) 2016/794, the European Union Agency for Law Enforcement Cooperation (Europol) is to process data in accordance with the rules set out therein. That Directive and that Regulation are 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 remain limited to the categories of data per category of data subject listed in Section B 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. Furthermore, as far as possible, any such personal data should be distinguished in accordance with their degree of accuracy and reliability. In order to ensure accuracy and reliability, facts should be distinguished from personal assessments. The Single Points of Contact or, where applicable, competent law enforcement authorities should process requests for information under this Directive as quickly as possible in order to ensure the accuracy and reliability of personal data, to avoid unnecessary duplication of data, and to reduce the risk of data becoming outdated or no longer being available to them. Where it appears that the personal data are incorrect, they should be rectified or erased or their processing should be restricted without delay.

(24) In order to allow for the adequate and rapid provision of information by Single Points of Contact, either upon request or on their own initiative, it is important that the competent law enforcement authorities understand each other. All exchanges of information, including the provision of requested information, refusals of requests for information, including the reasons for such refusals, and, where applicable, requests for clarification or specifications and clarification or specifications provided which relate to a specific request should be transmitted in the language in which that request was submitted. Therefore, to prevent delays in the provision of requested information caused by language barriers and to limit translation costs, Member States should establish a list of one or more languages in which their Single Point of Contact can be addressed and in which it can communicate. Since English is a language that is broadly understood and used in practice with regard to law enforcement cooperation within the Union, it should be included on that list. Member States should provide that list and any updates thereto to the Commission. The Commission should publish online a compilation of those lists.

([17]) 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).

(25) To ensure the safety and security of European citizens, it is essential that Europol hold the necessary information to fulfil its role as the Union's criminal information hub supporting the competent law enforcement authorities. Therefore, when information is exchanged between Member States, irrespective of whether it is exchanged pursuant to a request for information submitted to a Single Point of Contact or competent law enforcement authority or whether it is provided by a Single Point of Contact or competent law enforcement authority on its own initiative, an assessment should be made, on a case-by-case basis, as to whether a copy of the request for information submitted under this Directive or of the information exchanged under this Directive should be sent to Europol in accordance with Article 7(6) of Regulation (EU) 2016/794 where it concerns a criminal offence falling within the scope of the objectives of Europol. Such assessments should be based on Europol's objectives as set out in Regulation (EU) 2016/794 in so far as the scope of the criminal offence is concerned. Member States should not be obliged to send a copy of the request for information or of the information exchanged to Europol where it would be contrary to the essential interests of the security of the Member State concerned, where it would jeopardise the success of an ongoing investigation or the safety of an individual or where it would disclose information relating to organisations or specific intelligence activities in the field of national security. Moreover, in accordance with the principle of data ownership and without prejudice to the obligation set out in Regulation (EU) 2016/794 concerning the determination of the purpose of, and restrictions on, the processing of information by Europol, 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. Member States should ensure that the staff of their Single Point of Contact and competent law enforcement authorities are adequately supported and trained to quickly and accurately identify which information exchanged under this Directive falls within the mandate of Europol and is necessary for it to fulfil its objectives.

(26) The problem of the proliferation of communication channels used for the transmission of law enforcement information between Member States should be remedied because 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 (SIENA), managed and developed by Europol in accordance with Regulation (EU) 2016/794, should be made mandatory for all transmissions and communications under this Directive, including the sending of requests for information to Single Points of Contact and directly to competent law enforcement authorities, the provision of information pursuant to such requests and the provision of information by Single Points of Contact and competent law enforcement authorities on their own initiative, communications on refusals of requests for information, clarification and specifications, and the sending of copies of requests for information or information to Single Points of Contact and Europol. To that end, all Single Points of Contact, and all competent law enforcement authorities that might be involved in exchanges of information, should be directly connected to SIENA. To allow frontline officers, such as police officers involved in dragnet operations, to use SIENA, it should also be operational on mobile devices, where appropriate. In that regard, a short transition period should be provided for in order to allow for the full roll-out of SIENA because it entails a change of the current arrangements in some Member States and requires those staff 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 Point of Contact or their competent law enforcement authorities to use another secure communication channel in a limited number of justified situations. Where Member States permit their Single Point of Contact or their competent law enforcement authorities to use another communication channel due to the urgency of the request for information, they should, where practicable and consistent with operational needs, revert to using SIENA after the situation ceases to be urgent. The use of SIENA should not be mandatory for internal exchanges of information within a Member State.

(27) In order to simplify, facilitate and better manage information flows, each Member State should establish or designate a Single Point of Contact. Single Points of Contact should be competent for coordinating and facilitating the exchange of information under this Directive. Each Member State should notify the Commission of the establishment or designation of its Single Point of Contact and any changes thereto. The Commission should publish those notifications and any updates thereto. The Single Points of Contact should, in particular, contribute to mitigating the obstacles to information flows resulting from the fragmentation of the way in which competent law enforcement authorities communicate with one another, in response to the growing need to jointly tackle cross-border crime, such as drug trafficking, cybercrime, trafficking in human beings, and terrorism. The Single Points of Contact should be assigned a number of specific, minimum tasks and have certain minimum capabilities so that they are able to effectively fulfil their coordinating functions in respect of the cross-border exchange of information for law enforcement purposes under this Directive.

(28) The Single Points of Contact should have access to all information available within their Member State, including by having user-friendly access to all relevant Union and international databases and platforms, in accordance with the arrangements specified in the applicable Union and national law. In order to be able to meet the requirements of this Directive, in particular those on time limits, the Single Points of Contact should be provided with adequate resources in terms of budget and staff, including adequate translation capabilities, and they should function around the clock. In that regard, having a front desk that is able to screen, process and channel incoming requests for information could increase their efficiency and effectiveness. Single Points of Contact should also have at their disposition, at all times, judicial authorities competent to grant necessary judicial authorisations. In practice, that can be done, for example, by ensuring the physical presence of such judicial authorities within the premises of the Single Point of Contact or the functional availability of such judicial authorities either within the premises of the Single Point of Contact or directly available on call.

(29) 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 staff from 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, police, customs and other competent law enforcement authorities responsible for preventing, detecting or investigating criminal offences and possible contact points for 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 represented in the Single Points of Contact. However, in the interest of effective coordination, at a minimum, the Single Points of Contact should be composed of representatives of the Europol national unit, the SIRENE Bureau and the Interpol National Central Bureau, as established by the relevant Union legal act or international agreement and notwithstanding that this Directive does not apply to the exchange of information specifically regulated by those Union legal acts.

(30) 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 Points of Contact should be offered, and 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 the Single Points of Contact and competent law enforcement authorities of other Member States needed for the application of the rules set out in this Directive. In that 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 the protection of personal data, law enforcement cooperation and the handling of 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), established by Regulation (EU) 2015/2219 of the European Parliament and of the Council ([18]), 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.

(31) 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. Member States should also consider joint training courses 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.

(32) 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.

([18]) Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA (OJ L 319, 4.12.2015, p. 1).

(33) It is necessary that the Single Points of Contact deploy and operate a single electronic case management system having certain minimum functions and capabilities in order 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 the exchange of information. It is desirable that the universal message format standard established by Regulation (EU) 2019/818 of the European Parliament and of the Council ([19]) be used in the development of the case management system.

(34) The rules set out in Directive (EU) 2016/680 apply to the processing of personal data in the case management system. Processing includes storage. In the interests of clarity and the effective protection of personal data, the rules set out in that Directive should be further specified in this Directive. In particular, as regards the requirement set out in Directive (EU) 2016/680 that personal data be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed, this Directive should specify 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 in so far 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 rules concerning time limits for storage and review set out in Directive (EU) 2016/680, the Single Point of Contact should regularly review whether those requirements continue to be met. For that purpose, a first review should take place at the latest six months after an 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 for 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, in particular Directive (EU) 2016/680.

(35) In order to assist Single Points of Contact and competent law enforcement authorities in the exchange of information under this Directive and to foster a common European police culture between Member States, the Member States should encourage practical cooperation among their Single Points of Contact and competent law enforcement authorities. In particular, the Council should organise meetings of the Heads of the Single Points of Contact at least on an annual basis to share experience and best practice regarding the exchange of information for the purposes of this Directive. Other forms of cooperation should include the drafting of manuals on law enforcement information exchange, the compilation of national fact sheets 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 the specificities of relevant legal frameworks and the organisation, as appropriate, of meetings between relevant Single Points of Contact.

(36) 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. That 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. Data required for that purpose should be automatically generated by the case management system and SIENA.

([19]) Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).

(37) The cross-border nature of transnational crime and terrorism requires Member States to rely on one another to prevent, detect or investigate such criminal offences. Since the objective of this Directive, namely ensuring adequate and rapid information flows between competent law enforcement authorities and to Europol, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, 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, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). 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 that objective.

(38) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and the Council ([20]) and delivered an opinion on 7 March 2022.

(39) This Directive builds upon the values on which the Union is founded, as set out in Article 2 TEU, 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, 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 respectively, as well as by Article 16 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 established by Directive (EU) 2016/680 and the European Data Protection Supervisor, where appropriate in accordance with their respective mandates.

(40) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, 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 shall, 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.

(41) Ireland is taking part in this Directive, in accordance with Article 5(1) of Protocol No 19 on the Schengen *acquis* integrated into the framework of the European Union, annexed to the TEU and to the TFEU, and Article 6(2) of Council Decision 2002/192/EC ([21]).

(42) 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 latters' association with the implementation, application and development of the Schengen *acquis* ([22]) which fall within the area referred to in Article 1, point H, of Council Decision 1999/437/EC ([23]).

(43) 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* ([24]) 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 2008/149/JHA ([25]).

([20]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

([21]) 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, p. 20).

([22]) OJ L 176, 10.7.1999, p. 36.

([23]) 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, p. 31).

([24]) OJ L 53, 27.2.2008, p. 52.

([25]) 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, p. 50).

(44) 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* ([26]) 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 2011/349/EU ([27]),

HAVE ADOPTED THIS DIRECTIVE:

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

(b) the provision by a Member State, on its own initiative, of relevant information to the 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 under this Directive and the information to be provided to the Single Points of Contact in relation to the exchange of information directly between the competent law enforcement authorities;

(d) the establishment or designation and the organisation, tasks, composition and capabilities of each Member State's Single Point of Contact, including on the deployment and operation of a single electronic case management system for carrying out their tasks under this Directive.

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

([26]) OJ L 160, 18.6.2011, p. 21.

([27]) 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, p. 1).

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

(a) obtain information by means of coercive measures;

(b) store information for the sole purpose of providing it to the 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 consent to 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 or 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, but excludes agencies or units dealing especially with national security issues and liaison officers seconded pursuant to Article 47 of the Convention implementing the Schengen Agreement;

(2) '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);

(3) 'serious criminal offence' means any of the following:

(a) an offence as referred to in Article 2(2) of Council Framework Decision 2002/584/JHA ([28]);

(b) an offence as referred to in Article 3(1) or (2) of Regulation (EU) 2016/794;

(4) 'information' means any content concerning one or more natural or legal persons, facts or circumstances relevant to competent law enforcement authorities for the purpose of carrying out their tasks under national law of preventing, detecting or investigating criminal offences, including criminal intelligence;

(5) 'information available' means directly accessible information and indirectly accessible information;

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

(7) 'indirectly accessible information' means information that a Single Point of Contact or a competent law enforcement authority of the Member State from which information is requested 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;

(8) 'personal data' means personal data as defined in Article 3, point (1), of Directive (EU) 2016/680.

([28]) 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).

Article 3

Principles regarding the exchange of information

Each Member State shall, in connection with all exchanges of information under this Directive, ensure that:

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

(b) the conditions for requesting information from 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 within that Member State ('principle of equivalent access');

(c) it protects information provided to its Single Point of Contact or competent law enforcement authorities that is marked as confidential in accordance with the requirements set out in its national law offering a similar level of confidentiality as the national law of the Member State that provided the information ('principle of confidentiality');

(d) where the requested information was initially obtained from another Member State or a third country, it only provides such information to another Member State or to Europol with the consent of, and in accordance with the conditions imposed on its use by, the Member State or third country that initially provided the information ('principle of data ownership');

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

CHAPTER II

EXCHANGE OF INFORMATION THROUGH SINGLE POINTS OF CONTACT

Article 4

Requests for information to Single Points of Contact

1. Member States shall ensure that requests for information submitted by their Single Point of Contact and, where their national law so provides, the designated law enforcement authorities to the Single Point of Contact of another Member State comply with the requirements set out in paragraphs 2 to 6.

Member States shall submit to the Commission a list of their designated law enforcement authorities. Member States shall inform the Commission where there are changes to that list. The Commission shall publish online a compilation of those lists and keep it up to date.

Member States shall ensure that where their designated law enforcement authorities submit a request for information to the Single Point of Contact of another Member State, at the same time, they send a copy of that request to their Single Point of Contact.

2. Member States may permit their designated law enforcement authorities not to send, on a case-by-case basis, a copy of a request for information to their Single Point of Contact at the same time as submitting it to the Single Point of Contact of another Member State in accordance with paragraph 1 where it would jeopardise one or more of the following:

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

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

(c) the safety of an individual.

3. Member States shall ensure that requests for information are submitted to the Single Point of Contact of another Member State only where there are objective reasons to believe that:

(a) the requested information is necessary for and proportionate to achieving the purpose referred to in Article 1(1), first subparagraph; and

(b) the requested information is available to that other Member State.

4. Member States shall ensure that any request for information submitted to the Single Point of Contact of another Member State specifies whether it is urgent and, if so, gives reasons for the urgency. Such requests for information shall be considered urgent where, 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 prevent an imminent threat to life or the physical integrity of a person;

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

(d) at imminent risk of losing relevance if not provided urgently and is considered important for the prevention, detection or investigation of criminal offences.

5. Member States shall ensure that requests for information submitted to the Single Point of Contact of another Member State contain all necessary 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 for which it is believed that the requested information is available to the requested Member State;

(d) an explanation of the connection between the purpose for which the information is requested and any natural or legal person or entity to which the information relates, where applicable;

(e) the reasons for which the request is considered urgent, where applicable, in accordance with paragraph 4;

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

6. Member States shall ensure that requests for information are submitted to the Single Point of Contact of another Member State in one of the languages included in the list established by that other Member State in accordance with Article 11.

Article 5

Provision of information pursuant to requests to Single Points of Contact

1. 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 in the case of urgent requests relating to directly accessible information;

(b) three calendar days in the case of urgent requests relating to indirectly accessible information;

(c) seven calendar days in the case of all other requests.

The time limits set out in the first subparagraph shall commence as soon as the request for information is received.

2. Where, under its national law in accordance with Article 9, a Member State can provide the requested information only after having obtained a judicial authorisation, that Member State may deviate from the time limits set out in paragraph 1 of this Article in so far as necessary for the purpose of obtaining such an authorisation. In such cases, Member States shall ensure that their Single Point of Contact does both of the following:

(a) 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 therefor;

(b) subsequently keep the Single Point of Contact, or where applicable, the designated law enforcement authority of the requesting Member State 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(6).

Member States shall ensure that their Single Point of Contact sends a copy of the requested information to the Single Point of Contact of the requesting Member State at the same time as providing the requested information to the designated law enforcement authority of that Member State.

Member States may 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 other Member State where it would jeopardise one or more of the following:

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

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

(c) the safety of an individual.

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 in so far as any of the following reasons applies:

(a) the requested information is not available to the Single Point of Contact and 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 those falling within the categories of personal data referred to in Article 10, point (b);

(e) 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;

(f) 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 protected important interests of a legal person;

(g) the request pertains to:

(i) a criminal offence punishable by a maximum term of imprisonment of one year or less under the law of the requested Member State; or

(ii) a matter that is not a criminal offence under the law of the requested Member State;

(h) the requested information was initially obtained from another Member State or a third country and that Member State or third country has not consented 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 set out in Article 4, in particular as to whether there is a manifest breach of fundamental rights.

Any refusal of a request for information shall affect only the part of the requested information to which the reasons set out in the first subparagraph relate and shall, where applicable, not affect the obligation to provide the other parts of the information in accordance with this Directive.

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 of the request for information, specifying the reasons therefor, within the time limits set out in Article 5(1).

3. Where relevant, Member States shall ensure that their Single Point of Contact immediately requests, from the Single Point of Contact or, where applicable, the designated law enforcement authority of the requesting Member State, clarification or specifications needed to process a request for information that otherwise would have to be refused.

The time limits set out 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 clarification or specifications until the moment the requested clarification or specifications are provided.

4. Refusals of requests for information, reasons for such refusals and requests for clarification or specifications and clarification or specifications as referred to in paragraph 3 of this Article, as well as any other communications relating to the requests for information submitted 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(6).

CHAPTER III

OTHER EXCHANGES OF INFORMATION

Article 7

Own-initiative provision of information

1. Member States may provide, on their own initiative, through their Single Point of Contact or through their competent law enforcement authorities, information available to it or 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 those other Member States for the purpose of preventing, detecting or investigating criminal offences.

2. Member States shall ensure that their Single Point of Contact or their competent law enforcement authorities provide, on its or their own initiative, information available to it or 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 those other Member States for the purpose of preventing, detecting or investigating serious criminal offences. However, no such obligation shall exist in so far as the reasons referred to in Article 6(1), point (c) or (f), apply in respect of such information.

3. Member States shall ensure that, where their Single Point of Contact or their competent law enforcement authorities provide information on its or their own initiative to the Single Point of Contact of another Member State in accordance with paragraph 1 or 2, they do so in one of the languages included in the list established by that other Member State in accordance with Article 11.

Member States shall ensure that, where their Single Point of Contact provides information on its own initiative to the competent law enforcement authority of another Member State, it 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 authorities provide information on their own initiative to another Member State, they send, at the same time, a copy of that information to the Single Point of Contact of their Member State and, where appropriate, to the Single Point of Contact of that other Member State.

4. Member States may 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 the Single Point of Contact of their Member State or to the Single Point of Contact of that other Member State where it would jeopardise one or more of the following:

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

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

(c) the safety of an individual.

Article 8

The exchange of information upon requests submitted directly to competent law enforcement authorities

1. Member States shall ensure that, where their Single Point of Contact submits a request for information directly to a competent law enforcement authority of another Member State, at the same time, it sends a copy of that request to the Single Point of Contact of that other Member State. Member States shall ensure that, where one of their competent law enforcement authorities provides information pursuant to such a request, it sends, at the same time, a copy of that information to the Single Point of Contact of its Member State.

2. Member States shall ensure that, where one of their competent law enforcement authorities submits a request for information or provides information pursuant to such a request directly to a competent law enforcement authority of another Member State, at the same time, it sends a copy of that request or that information to the Single Point of Contact of its Member State and to the Single Point of Contact of that other Member State.

3. Member States may permit their Single Point of Contact or competent law enforcement authorities not to send copies of requests or information as referred to in paragraph 1 or 2 where it would jeopardise one or more of the following:

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

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

(c) the safety of an individual.

CHAPTER IV

ADDITIONAL RULES ON THE PROVISION OF INFORMATION UNDER CHAPTERS II AND III

Article 9

Judicial authorisation

1. A Member State shall not require a judicial authorisation in order to provide information to the Single Point of Contact or to the competent law enforcement authorities of other Member States under Chapter II or III where its national law does not require such a judicial authorisation for providing similar information within that Member State.

2. Member States shall ensure that, where a judicial authorisation is required under their national law in order to provide information to the Single Point of Contact or to the competent law enforcement authorities of other Member States under Chapter II or III, their Single Point of Contact or their competent law enforcement authorities immediately take all the necessary steps, in accordance with their national law, to obtain such a judicial authorisation as soon as possible.

3. Requests for judicial authorisation as referred to in paragraph 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 Chapter II or III that constitutes personal data:

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

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

(c) their Single Point of Contact or their competent law enforcement authorities also provide, at the same time and 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 and 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 indicating one or more of the languages in which their Single Point of Contact is able to exchange information. That list shall include English.

2. Member States shall provide the list referred to in paragraph 1 and any updates thereto to the Commission. The Commission shall publish online a compilation of those lists and keep it up to date.

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 or provide information on its or their own initiative under Chapter II or III of this Directive, the staff of their Single Point of Contact or competent law enforcement authorities also assess, on a case-by-case basis and subject to Article 7(7) of Regulation (EU) 2016/794, whether it is necessary to send a copy of the request for information or of the information provided to Europol, in so far as the information to which the communication relates concerns criminal offences falling within the scope of the objectives of Europol set out in Article 3 of Regulation (EU) 2016/794.

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

Article 13

Secure communication channel

1. Member States shall ensure that their Single Point of Contact or their competent law enforcement authorities use Europol's Secure Information Exchange Network Application (SIENA) to send requests for information, to provide information pursuant to such requests or to provide information on its or their own initiative under Chapter II or III or under Article 12.

2. Member States may permit their Single Point of Contact or their competent law enforcement authorities not to use SIENA to send requests for information, to provide information pursuant to such requests or to provide information on its or their own initiative under Chapter II or III or under Article 12 in one or more of the following cases:

(a) the exchange of information requires the involvement of third countries or international organisations or 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 for information requires the temporary use of another communication channel;

(c) an unexpected technical or operational incident prevents their Single Point of Contact or their competent law enforcement authorities from using SIENA to exchange the information.

3. Member States shall ensure that their Single Point of Contact, and all their competent law enforcement authorities that might be involved in the exchange of information under this Directive, are directly connected to SIENA, including, where appropriate, through mobile devices.

CHAPTER V

SINGLE POINT OF CONTACT FOR THE EXCHANGE OF INFORMATION BETWEEN MEMBER STATES

Article 14

Establishment or designation and tasks and capabilities of Single Points of Contact

1. Each Member State shall establish or designate a Single Point of Contact. The Single Point of Contact shall be the central entity responsible for coordinating and facilitating the exchange 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) receiving and evaluating requests for information submitted in accordance with Article 4 in the languages notified pursuant to Article 11(2);

(b) channelling requests for information to the relevant competent law enforcement authorities and, where necessary, coordinating among them the processing of such requests and the provision of information pursuant to such requests;

(c) coordinating the analysis and 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) providing, on request or on its own initiative, information to other Member States in accordance with Articles 5 and 7;

(e) refusing to provide information in accordance with Article 6 and, where necessary, requesting clarification or specifications in accordance with Article 6(3);

(f) sending requests for information to the Single Points of Contact of other Member States in accordance with Article 4 and, where necessary, providing clarification or specifications in accordance with Article 6(3).

3. Member States shall ensure that:

(a) their Single Point of Contact:

(i) has access to all information available to their competent law enforcement authorities, in so far as necessary to carry out its tasks under this Directive;

(ii) carries out its tasks 24 hours a day, 7 days a week;

(iii) is provided with 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, within the time limits set out in Article 5(1);

(b) 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. Member States shall notify the Commission within one month of the establishment or designation of their Single Point of Contact. They shall inform the Commission where there are changes as regards their Single Point of Contact.

The Commission shall publish those notifications, and any updates thereto, 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 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 staff from 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 in so far as the Member State concerned is bound by the relevant law 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;

(c) the Interpol National Central Bureau established by Article 32 of the Constitution of the International Criminal Police Organisation – Interpol.

3. Member States shall ensure that the staff of their Single Point of Contact are adequately qualified in order to carry out their functions under this Directive. To that end, Member States shall provide the staff of their Single Point of Contact 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 a single electronic 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 as referred to in Articles 5 and 8 and any other communications relating to such requests with Single Points of Contact and, where applicable, the competent law enforcement authorities of other Member States, including information about refusals of requests for information and requests for and the provision of clarification or specifications as referred to in Article 6(2) and (3) respectively;

(b) recording communications between the Single Point of Contact and the competent law enforcement authorities, pursuant to Article 14(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 as referred to in Articles 5 and 8 against information available to the Single Point of Contact, including information provided in accordance with Article 5(3), second subparagraph, and Article 7(3), second subparagraph, and other relevant information recorded in the case management system;

(e) ensuring adequate and rapid follow-up to incoming requests for information as 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 purposes of Article 18;

(h) logging access and other processing operations 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 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 personal data 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 contained therein are subsequently irrevocably deleted.

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

Article 17

Cooperation between Single Points of Contact

1. Member States shall encourage practical cooperation between their Single Points 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 18

Statistics

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

2. Each Member State shall ensure that the statistics referred to in paragraph 1 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 that their Single Point of Contact and their competent law enforcement authorities received and the number of requests for information to which they replied, broken down by urgent and non-urgent requests and by requesting Member State;

(c) the number of requests for information refused pursuant to Article 6, broken down by requesting Member State and by ground for refusal;

(d) the number of cases in which there was a deviation from the time limits set out in Article 5(1) because it was necessary to obtain a judicial authorisation in accordance with Article 5(2), broken down by the Member States that submitted the requests for information concerned.

3. The Commission shall compile the minimum statistics provided by Member States under paragraph 2 and make them available to the European Parliament and to the Council.

Article 19

Reporting

1. The Commission shall, by 12 June 2026 and every five years after 12 June 2027, submit a report to the European Parliament and to the Council assessing the implementation of this Directive and containing detailed information on how each Member State has implemented this Directive. In compiling that report, the Commission shall pay particular attention to how efficiently competent law enforcement authorities exchanged information, the grounds for which requests for information were refused, in particular where requests fall outside the scope of the objectives of this Directive, and the compliance with provisions on data protection and the provision of information to Europol.

2. The Commission shall, by 12 June 2027 and every five years thereafter, submit a report to the European Parliament and to the Council assessing the effectiveness of this Directive, in particular its impact on law enforcement cooperation, the obligations laid down in Article 14(3), point (a)(iii), 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 that assessment, the Commission shall decide on appropriate follow-up actions, including, where appropriate, a legislative proposal.

Article 20

Amendments to the Convention implementing the Schengen Agreement

From 12 December 2024, the parts of Articles 39 and 46 of the Convention implementing the Schengen Agreement that have not been replaced by Framework Decision 2006/960/JHA are replaced by this Directive in so far as those Articles relate to the exchange of information falling within the scope of this Directive.

Article 21

Repeal

Framework Decision 2006/960/JHA is repealed from 12 December 2024.

References to the repealed Framework Decision shall be construed as references to this Directive and shall be read in accordance with the correlation table in the Annex.

Article 22

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 12 December 2024. They shall immediately inform the Commission thereof.

By way of derogation from the first subparagraph, Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with Article 13 by 12 June 2027. They shall immediately inform the Commission thereof.

When Member States adopt the measures referred to in the first and second subparagraphs, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

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

Article 23

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 24

Addressees

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

Done at Strasbourg, 10 May 2023.

For the European Parliament	*For the Council*
The President	*The President*
R. METSOLA	J. ROSWALL

ANNEX

CORRELATION TABLE

Council Framework Decision 2006/960/JHA	This Directive
Article 1	Article 1
Article 2	Article 2
Article 3	Articles 3 and 9
Article 4	Article 5
Article 5	Article 4
Article 6	Articles 11, 12 and 13
Article 7	Articles 7 and 8
Article 8	Article 10
Article 9	Article 3
Article 10	Article 6
Article 11	Article 21
Article 12	Article 19
Article 13	Article 22