EUROPEAN
COMMISSION

Brussels, 8.12.2021
COM(2021) 782 final

2021/0411 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA

{SEC(2021) 420 final} - {SWD(2021) 374 final} - {SWD(2021) 377 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• General context

As set out in the EU Security Union Strategy[1], the new Counter-terrorism agenda for the EU[2] and the EU Strategy to tackle Organised Crime 2021-2025[3], transnational threats call for a coordinated, more targeted and adapted response. While national authorities operating on the ground are on the frontline in the fight against organised crime and terrorism, action at Union level and global partnerships are paramount to ensure effective cooperation as well as information and knowledge exchange among national authorities, supported by a common criminal law framework and effective financial means. Furthermore, organised crime and terrorism are emblematic of the link between internal and external security. These threats spread across borders and manifest themselves in organised crime and terrorist groups that engage in a wide range of criminal activities.

In an area without internal border controls ('the Schengen area'[4]), police officers in one Member State should have equivalent access to the information available to their colleagues in another Member State (subject to the same conditions). They should cooperate effectively and by default across the Union. Exchange of information on criminal matters is thus a key enabler to safeguarding security in the Schengen area.

Together with the abolition of internal border controls within the Schengen area, a set of rules for information exchange and police cooperation were agreed upon in the Convention Implementing the Schengen Agreement (CISA). In addition, the Schengen Information System (SIS) was established, creating a common EU security and border database containing information on wanted and missing persons and objects in the forms of alerts.

According to the EU Serious and Organised Crime Threat Assessment 2021 (EU SOCTA), more than 70% of organised crime groups are present in more than three Member States[5]. The 2021 EU SOCTA and the EMCDDA European Drug report[6] outline a number of areas where serious and organised crime appears to be on the rise. At the same time, as set out in the December 2020 Counter-Terrorism Agenda[7], the EU remains on high terrorist alert.

The Schengen area is the largest free travel area in the world. It allows more than 420 million people to move freely and goods and services to flow unhindered. By removing border controls between Member States, the Schengen area has become part of our European way of life. It is a symbol of Europe's interconnectedness and of the ties between European citizens[8]. The Schengen area also contributes to the efficient functioning of the Single Market, and thus to the growth of the Union's economy[9].

---

1 COM(2020) 605 final.
2 COM(2020) 795 final.
3 COM(2021) 170 final.
4 The Schengen area is composed of Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden and Switzerland.
5 Europol (2021), European Union *Serious and Organised Crime Threat Assessment (EU SOCTA).*
6 European Monitoring Centre for Drugs and Drug Addiction *(*EMCDDA), *European drug report 2021*.
7 COM(2020) 795 final.
8 Eurobarometer 474: *The Schengen Area*.
9 COM(2021) 277 final, 2.6.2021.

However, the growing mobility of people within the EU also creates additional challenges in preventing and fighting criminal threats, and in ensuring public safety. Almost 2 million people commuted across borders, including 1.3 million cross-border workers[10]. Despite the COVID-19 pandemic having reduced intra-EU mobility, flows of people will likely continue to be important in the future.

In recent years, the Schengen area has been repeatedly put to the test by a series of crises and challenges which have led several Member States to reintroduce internal border controls. One reason Member States have given for such a decision has been the uncontrolled secondary movements[11] of irregular migrants, which these Member States consider to pose a serious threat to public policy or internal security, justifying the need to reintroduce border controls. Pursuant to Regulation (EU) 2016/399[12] ('Schengen Borders Code'), the temporary reintroduction of border controls may be used only for a limited period of time, in exceptional circumstances (such as the migratory crisis observed in 2015/2016), as a last resort measure. In particular, there is room for improvement as regards the use of police checks and cooperation, including of course with regard to information exchange and communication. These measures, in particular if combined, have the potential to yield the same results in controlling secondary movements as temporary internal border controls, and are less intrusive when it comes to the free movement of persons, goods and services.

The rapidly evolving criminal landscape and the mobility of people suggest that cross-border cooperation between law enforcement authorities in the EU and the Schengen area is crucial to tackle criminal offences, and allow citizens and third country nationals legally staying on the territory to safely use their free movement. However, important challenges remain for law enforcement authorities' ability to exchange information with their counterparts in other Member States in an effective and efficient manner. This capability still varies greatly among the Member States highlighting a degree of fragmentation detrimental to the effectiveness and efficiency of information exchange. As a result, criminals and groups of criminals continue to take advantage of these inefficiencies to operate across borders, and secondary movements of irregular migrants will continue to pose a problem.

• Reasons for and objectives of the proposal

The overall objective of this proposal is to legislate on organisational and procedural aspects of information exchange between law enforcement authorities in the EU with a view to contributing to the effective and efficient exchange of such information, hence protecting a fully functioning and resilient Schengen area. The proposal is (notably) without prejudice to the rules regulating the information exchange on alerts in the SIS via the Supplementary Information Request at the National Entries (SIRENE) Bureaux.

This proposal for a *Directive on information exchange between law enforcement authorities of Member States* forms part of a coherent package also comprising a proposal for a Council Recommendation reinforcing operational cross-border police cooperation, a proposal for a Regulation revising the Automated Data Exchange Mechanism for Police Cooperation ("Prüm II") as well as a proposal amending the Schengen Borders Code as set out in the Commission Communication of June 2021 "*A strategy towards a fully functioning and resilient Schengen area*"[13]. Together, these proposals seek to establish a Police Cooperation Code with the

10 European Commission (2017), *Boosting Growth and cohesion in EU border regions*.

11 Other most frequent reasons notified by the Member States included the migratory crisis of 2015/2016, persistent terrorist threat and the COVID-19 pandemic.

12 Regulation (EU) 2016/399 (Schengen Borders Code).

13 COM(2021) 277 final, 2.6.2021.

objective of streamlining, enhancing, developing, modernising and facilitating law enforcement cooperation between relevant national agencies, thus supporting Member States in their fight against serious and organised crime and terrorism.

Taking full account of the opinion expressed by the co-legislator, this proposal is based on the findings presented in the accompanying Impact Assessment. These findings also cover information, analyses and recommendations stemming from the Schengen evaluations in the field of police cooperation carried out in the past six years, the Communiction from the Commission on the way forward on aligning the former third pillar *acquis* with data protection rules[14], the extensive consultations with relevant stakeholders in the past two years, and the important body of Council guidance papers developed for the last 15 years. Based on this combined analysis, three main objectives were identified. The present proposal seeks to achieve them by addressing three underlying problems.

(1) Lack of clear and robust common rules on information exchange

The first objective of this proposal is to ensure, under precise, consistent and common rules, **the equivalent access for any Member State's law enforcement authorities to information available in other Member States** for the purpose of preventing and detecting criminal offences, conducting criminal investigations or criminal operations, **while complying with fundamental rights, including data protection requirements.**

Member States' Law Enforcement Authorities (LEAs) are involved in daily cross-border information exchanges related to operations against criminal offences. **Yet, rules at national level impede the effective and efficient flow of information**. The general rules for the exchange of law enforcement information which has cross-border relevance among Member States' law enforcement authorities are laid down in Council Framework Decision 2006/960/JHA simplifying the exchange of information between law enforcement authorities of the Member States of the European Union (hereinafter referred to as 'Swedish Framework Decision' or 'SFD'[15]), adopted in 2006 before the entry into force of the Treaty of Lisbon. The Swedish Framework Decision partially superseded the police cooperation Chapter of the 1990 Convention Implementation the Schengen Agreement[16].

The Swedish Framework Decision lays down the **principles** according to which information should be shared (principles of availability and equivalent access), the **timeframe** within which a request for information should be replied to, the **forms** that should be used to lodge and reply to such requests, as well as the data protection **safeguards** to be ensured when handling these information.

In practice, however, the 2006 Swedish Framework Decision is unclear, thereby hampering the full implementation of the principles of availability/equivalent access of relevant information in a cross-border context[17]. As a consequence, rules at national level continue to impede the flow of information despite the efforts made to complement the Swedish Framework Decision requirements by means of Council non-binding guidance[18].

---

14 COM(2020) 262 final, 24.6.2020.

15 OJ L 386, 29.12.2006, p. 89–100.

16 OJ L 239, 22.9.2000, p. 19–62.

17 These outstanding issues have notably been highlighted in the Schengen evaluations in the field of police cooperation. These country report evaluations underline the existence of diverging practices depending on the other State party. They also cover relevant Council guidance papers and the police cooperation chapter of the 1990 Convention Implementing the Schengen Agreement and their related bi/multilateral agreements.

18 For example: Council doc. 5825/20 of 2/12/2020, *Manual on Law Enforcement Information Exchange*.

Consequently, the current uncertainties would remain and continue to negatively affect the effective and efficient sharing of information, thereby leaving the impacts in the evolution of the EU security landscape and in the increased cross-border mobility essentially unaddressed.

For this reason, establishing a legal framework by means of a Directive for these purposes will allow a better monitoring and enforcement of rules at EU and national levels, while ensuring a convergence of national practices, thereby improving the effectiveness and efficiency of information flows between Member States.

(2) Lack of common structures and efficient management tools for exchanging information

The second objective of this proposal for a Directive is to approximate common minimum standards with a view to ensuring an efficient and effective functioning of the Single Points of Contact. These common minimum requirements cover the composition, structures, responsibilities, staffing and technical capabilities.

Member States are responsible for the maintenance of law and order and the safeguarding of internal security[19]. They are in principle free to organise their law enforcement authorities and services as they see fit. When it comes to law enforcement cooperation structures, all Member States have set up or are in the process of setting up a Single Point of Contact[20] competent for channelling as much information exchange as possible. Based on national law or internal rules, law enforcement authorities may also exchange information directly between themselves. Although different manuals and national factsheets have been produced in order to facilitate a harmonised approach to the way national Single Points of Contact are organised, there are still significant differences across Member States as regards their structures, functions, means and capabilities.

As a result, **Member States do not always have the necessary structures in place to exchange information effectively and efficiently with other Member States**. National Single Points of Contact do not always play their coordination role and can lack resources to face the increasing number of requests.

Notably, they are not always equipped with the necessary information management tools (for example, a case management system with a common dashboard and automatic data upload and cross-check). Additionally, the **Single Points of Contact do not always have direct and user-friendly access to all relevant EU and international databases** and platforms. Moreover, some Single Points of Contact have limited access to **relevant national databases**, which further delays the overall information exchange process. Furthermore, the Single Points of Contact can lack resources to timely and effectively address the increasing number of requests received. Indeed, this rising trend has not always been accompanied by a proportionate increase of human and IT resources.

A modern information management architecture, already in use in some 'advanced' Single Points of Contact, can alleviate tensions on limited human resources through the integration of information held by competent authorities in their respective databases, thereby also monitoring and tracking the deadline for answers to information requests[21]. Databases

---

19 Article 72 TFEU.

20 The Single Point of Contact is the national information hub centralising the reception, processing and the sending of the information to other countries. It gathers under the same management structure all main international and EU law enforcement communication channels (INTERPOL, Europol and SIRENE).

21 See the Impact Assessment accompanying this proposal.

available at Single Points of Contact are not always used to their full potential either because of **rudimentary search tools,** preventing the adoption of transliteration[22] techniques and "fuzzy logic"[23] search functions. The lack of transliteration and fuzzy logic search options within information systems prevents officials from getting exhaustive results (hits) through a unique query. As a result, officials have to carry out a new search for each personal detail they are investigating, resulting in an increased workload, which slows down the search process (for example, inversion of first and last name, different spelling used for the same individual notably stemming from different languages, alphabets and diacritic accents).

At present, deadlines are almost always exceeded when a judicial authorisation is required. The **functional availability of a judicial authority**, as it is already the case in more effective and efficient Single Points of Contact, will contribute to alleviate undue delays. Indeed, cases requiring a judicial authorisation can be handled more swiftly than what is currently the case, meaning that deadlines can be more readily met also in these cases.

(3) Lack of common practice in the use of existing communication channel(s) to exchange information within the EU

The third objective of this proposal for a Directive is to **remedy the proliferation of communication channels used for law enforcement information exchange between Member States while reinforcing Europol's role as the EU criminal information hub for offences falling within its mandate.**

Besides a number of system-specific cases regulated by EU law (i.e. requests for supplementary information related to SIS alerts must be made via SIRENE Bureaux[24], and information exchange with Europol usually via ENUs[25]), Member States have not agreed on a single channel of information exchange between their law enforcement authorities for cases with an EU dimension, leading to duplication of requests, undue delays and occasional information loss.

As a result, Member States use different channels to different extents to request, send and receive information, often without any clear, pre-defined rationale[26], which hampers effective and efficient exchange of information. This also deprives national authorities from Europol's support even though Member States call on the Agency to be an EU criminal information hub able to deliver qualitative information-led products.

Single Points of Contact do not always ensure the monitoring of existing channels 24/7 resulting in possible negative impacts on cross-border cases requiring urgent information sharing. At the same time, Europol's Secure Information Exchange Network Application (hereinafter 'SIENA') is being underused in spite of its tailored features and strong data security infrastructure. Even when Member States do use SIENA, they **do not always involve**

---

22 Transliteration is the process of representing words/names from one language using the alphabet or writing system of another language (multilingual name recognition). E.g. the letter "o" can be 'ò', 'ó', 'ô, 'õ', 'ö', 'ø' depending on the language/alphabet used.

23 A fuzzy database is a database which is able to deal with uncertain or incomplete information using fuzzy logic. i.e. the ability to find matches even when a person' name is misspelled.

24 The exchange of supplementary information related to SIS alerts must be done via a single network of national offices called SIRENE Bureaux.

25 Europol National Unit. Information exchange with Europol must be done via ENUs using SIENA.

26 A number of national SPOCs use internal guidelines recommending or requiring the specific use of a communication channel for specific purpose, thereby ensuring consistency and avoiding duplication of requests. However, other SPOCs rely on officers' habits and preferences, such leeway resulting in inefficiencies in a cross-border investigation context.

(by copying in) Europol, even though the information exchanged falls within its mandate. This can create significant information gaps at EU level.

- **Consistency with existing policy provisions in the policy area**

The present proposal is consistent with existing and upcoming policy provisions in the domain of law enforcement cooperation. Law enforcement cooperation is an area of shared competence between the EU and the Member States. In recent years, progress was made to improve the exchange of information cooperation between Member States and to close down the space in which terrorists and serious criminals operate. The legislative framework on counterterrorism and information exchange was strengthened in the aftermath of the terrorist attacks in Europe. Following the migration crisis of 2015, the general architecture of Justice and Home Affairs (JHA) information systems and databases was overhauled with a focus on interoperability[27] and dynamic convergence between security, borders and migration management. Moreover, greater cooperation between law enforcement bodies was promoted at EU level through the publication of (non-binding) Council recommendations and guidelines seeking to facilitate the convergence of national practices.

As the two legs of law enforcement cooperation essentially relate to (i) information exchange (which is the focus of the present proposal), and (ii) operational cross-border cooperation, the present proposal will form part of a coherent package with the accompanying proposal for a Council Recommendation on aspects of cross-border operational police cooperation. This package is complemented with the parallel proposal for a Regulation revising the Automated Data Exchange Mechanism for Police Cooperation ("Prüm II"). The "Prüm II" proposal will aim at strengthening the technical architecture of the Prüm exchange, broadening its scope of data categories and streamlining and accelarating its post-hit data exchange. The reinforced "Prüm II" proposal would provide specific rules and possibilities for the **automated** exchange of specific – and particularly important – data categories (for example, fingerprints, DNA, facial images) within the overall framework and general rules for general information exchange that this Directive will provide.

As an important measure to enhance security within the EU, the present proposal will also contribute to a fully functioning and resilient Schengen area as set out in the Schengen Strategy. This proposal is also in full coherence with the 2020 proposal revising the Europol mandate[28] with a view to strenghening the agency's mandate on processing large and complex datasets as well as with the European Production and Preservation Orders for electronic evidence in criminal matters[29]. The proposal complements the legal framework[30] on the

---

27 Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between the EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA [2019] OJ L 135/27; Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between the 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 [2019] OJ L 135/85.

28 COM/2020/796 final.

29 COM/2018/225 final - 2018/0108 (COD).

30 OJ L 312, 7.12.2018, p. 1–13. Regulation 2018/1860 on the use of the Schengen Information System for the return of illegally staying third-country nationals; Regulation 2018/1861 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation No 1987/2006; Regulation 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in

exchange of information on alerts in the SIS through the SIRENE Bureaux. This proposal is without prejudice to all those other acts of Union law, as well as other ones such as Directive 2019/1153 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 for the purpose of facilitating access to and the use of financial information and bank account information by competent authorities for the prevention, detection, investigation or prosecution of serious criminal offences[31].

- **Consistency with other Union policies**

The present proposal aims to contribute positively to a fully functioning and resilient Schengen area, allowing more people to move freely, and goods and services to flow unhindered, which in turn contributes to the efficient functioning of the Single Market, and thus to the growth of the Union's economy. The present proposal is therefore fully consistent with other Union policies in the field of employment, transport, and ultimately economic growth in intra-EU border regions, but also across the entire EU.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The legal basis for EU action in the field of intra-EU law enforcement cooperation is Title V, Chapter 5 of the Treaty on the Functioning of the European Union (TFEU). Pursuant to Article 87 TFEU: "*the Union shall establish police cooperation involving all the Member States' competent authorities, including police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences*". More specifically, Article 87(2)(a) TFEU relates to measures concerning the collection, storage, processing, analysis and exchange of information relevant for the prevention, detection and investigation of criminal offences. The present legal proposal is to be adopted according to the ordinary legislative procedure.

- **Subsidiarity (for non-exclusive competence)**

EU action is needed to properly address the problems identified in the first section of this explanatory memorandum. The objective of improving information flows between relevant law enforcement authorities and with Europol cannot be sufficiently achieved by the Member States acting alone. Owing to the cross-border nature of crime and terrorism, the Member States are obliged to rely on one another. Hence, the establishment of common rules for the exchange of information can be better achieved at the Union level. Despite the existence of a number of national and regional measures in place, Member States alone would not be able to ensure the full implementation of the principles of availability and of equivalent access to information. If acting alone and on the basis of national schemes, Member States would not overcome current differences among Single Points of Contact, which hinder the efficient and effective exchange of relevant information across borders. They would not ensure an appropriate and uniform level of knowledge of, and capacity in, the use of relevant databases and communication channels.

The EU is better equipped than individual Member States to ensure the coherence of actions taken at national level, address the divergence of national practices, prevent duplications, overlaps and uncertainties and eventually facilitate an efficient counter-action to cross-border

---

criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation No 1986/2006 and Commission Decision 2010/261/EU, as amended.

[31] OJ L 186, 11.7.2019, p. 122–137.

crime and terrorism. EU action, in response to the identified problems, is expected to bring added value for the entire EU, and therefore to its citizens, as it will render more resilient and robust the Schengen area, with a ripple effect on Schengen Associated Countries[32]. Common EU level rules, standards and requirements facilitating information exchange on cross-border crime between law enforcement authorities will generate significant economies of scale while ensuring high-level data security and data protection standards.

Law enforcement cooperation at EU level does not replace national policies on internal security. It does not substitute the work of national law enforcement authorities. Instead, EU level action supports and reinforces national security policies and the work of national law enforcement authorities against cross-border crime and terrorism.

- **Proportionality**

The present proposal aims to consolidate the EU legal framework in a single legal instrument on information exchange through the 'lisbonisation' of the Swedish Framework Decision. It also contains provisions stemming from a set of Council non-binding guidelines adopted over the past 15 years. Considering the call of the co-legislator and the willingness expressed by Member States in the consultation phase, this proposal for a Directive addresses the identified problems without going beyond what is strictly necessary to achieve the objective of ensuring effective and efficient information flows between Member States.

- **Choice of the instrument**

Building on previous relevant Council Conclusions[33], the present Commission proposal for a Directive aims to achieve effective and efficient information flows between law enforcement authorities of the Member States, by means of a substantial approximation of Member States' legislation concerning information exchange and communication. Its provisions ensure the respect of the conferral of powers as well as the differences in the legal systems and traditions of the Member States, as acknowledged by the Treaties. In light of the above, the proposed legal proposal takes the form of a Directive.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Stakeholder consultations**

The consultation involved **relevant stakeholders** from a wide range of subject matters, national police, customs, judicial and data protection authorities, civil society organisations, academia, and from members of the public on their expectations and concerns relating to strengthening law enforcement cooperation in the EU[34].

The Commission used different **means of engagement** such as targeted questionnaires, experts' interviews, focus groups, case-studies, and organised thematic workshops with Member States and Schengen Associated Countries' representatives. The subject matters and the policy options presented in the Impact Assessment accompanying the present proposal were also discussed within the relevant Council's Working Parties (for example, Law Enforcement Working Party/Police, Law Enforcement Working Party/Customs, Standing Committee on Operational Cooperation on Internal Security).

---

32 Iceland, Liechtenstein, Norway and Switzerland.

33 Council Conclusions on Internal Security and European Police Partnership, 13083/1/20.

34 An exhaustive presentation of the stakeholder consultations is found in the Impact Assessment accompanying the present proposal.

In addition, in line with the Better Regulation Guidelines[35], the Commission launched a **Public Consultation**. The **results of the consultation activities** (20 answers) have been duly taken into account in the preparation of the present proposal[36].

- **Collection and use of expertise**

Numerous consultation activities – such as scoping interviews, questionnaires and online surveys, semi-structured interviews, case-studies and focus groups – were also conducted by the contractor during the preparation of a '*Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation*'.

- **Impact assessment**

In line with the Better Regulation guidelines, an Impact Assessment was carried out for the preparation of the present legislative proposal. Based on its findings, the Commission identified three main problems which corresponds to three main specific objectives of the present proposal (as mentioned above). Correspondingly, three policy options with different degrees of intervention were considered for potentially achieving each of the specific objectives[37].

Specific objective 1: *Facilitate equivalent access for law enforcement authorities to information held in another Member State, while complying with fundamental rights, including data protection requirements.*

Through:

(1) ensuring alignment of the provisions currently contained in the 2006 SFD with the 2016 Data Protection Law Enforcement Directive;

(2) developing a set of new flanking 'soft' measures, such as training and Commission guidance on specific aspects law enforcement information exchange, as appropriate;

(3) improving the clarity of the SFD provisions. This is done through a clarification on the SFD scope and a simplification of its use. Commission guidance on the national datasets available in each Member States for possible exchange may also be developed to further improve implementation, as appropriate;

(4) facilitating compliance with deadlines requirements by which information is to be made available to another Member State, including when a judicial authorisation is required.

Specific objective 2: *Ensure that all Member States have an effective functioning Single Point of Contact, including when a judicial authorisation is required to provide information upon request of another Member State.*

Through:

(1) developing a new set of flanking 'soft' measures, such as training, financial support and Commission guidance of relevance, as appropriate;

(2) establishing minimum common requirements on the composition of the Single Points of Contact (including when a judicial authorisation is required), their functions, staffing, capabilities.

---

35 SWD (2017) 350, 7.7.2017.

36 EU police cooperation code – tackling cross-border serious & organised crime (europa.eu)

37 See Impact Assessment accompanying this proposal.

Specific objective 3: *Remedy the proliferation of communication channels used for law enforcement information exchange between Member States, while reinforcing Europol's role as the EU criminal information hub for offences falling within its mandate.*

Through:

(1) developing new set of flanking 'soft' measures, such as training, financial support and Commission guidance on information sharing, as appropriate;

(2) requiring Member States to use SIENA for all bi- and multilateral information exchanges under the proposed Directive after a necessary transition period ensuring the full roll-out of SIENA.

These measures will **streamline, clarify, develop and modernise cross-border law enforcement cooperation, while better safeguarding fundamental rights** in particular as regards the protection of personal data (as explained below). It will also step up Europol support to Member States in countering evolving threats. The preferred policy option will ensure a strong convergence of national practices regarding the effective and efficient functionning of Single Point of Contact, through common minimum standards.

The most positive impacts of the preferred policy option are expected to stem from establishing the Single Point of Contact as a "one-stop shop" for law enforcement cooperation in all Member States. The establishment of Europol SIENA as the default channel of communication will add to the streamlining of law enforcement information exchange, while ensuring the convergence of information at Europol, and the security of such information (and personal data). The preferred policy option also contains flanking measures such as relevant trainings and financial support, key enablers to achieving the specific objectives presented above. The preferred option reflects the best cumulative impacts as regards to relevance, added value, effectiveness, efficiency, coherence and proportionality. It draws lessons from the past and, at the same time, is sufficiently ambitious. The preferred option takes duly account of the views expressed by the Member States while responding to the legitimate expectations of the EU citizens and businesses. In doing so, the preferred option contributes to the effective and efficient functioning of the Schengen area.

- **Fundamental rights**

The Impact Assessment accompanying the present proposal analysed the effects that each policy options, including the measures envisaged by this proposal for a Directive, potentially have on fundamental rights of citizens. By definition, any policy options addressing information sharing between law enforcement authorities, have an impact on the right to protection of personal data, as provided for by Article 8 of Charter of Fundamental Rights of the EU (hereinafter: Charter) and Article 16 of the Treaty on the Functioning of the European Union.

The policy options also have a potential impact on other fundamental rights, such as those protected by Articles 2 (Right to life), 3 (Right to the integrity of the person), 6 (Right to liberty and security), 17 (Right to property) and 45 (Freedom of movement and of residence) of the Charter. The Impact Assessment considered that the chosen policy options are proportionate since they are limited to what is strictly necessary to meet the objective of safeguarding the internal security in the Schengen area while protecting the free movement of persons[38].

[38] See Impact Assessment accompanying this proposal.

Furthermore, the alignment of the relevant rules on exchanges of information for law enforcement purposes with the subsequently adopted and applicable rules on processing personal data for law enforcement purposes (pursuant to the 2016 Law Enforcement Data Protection Directive; hereinafter: LED[39]) are expected to positively impact safeguarding citizens' fundamental rights. The use of SIENA as the communication channel will also enhance the security of the personal data processing systems and their overall protection against possible abuses. As the LED provides and ensures the required level of personal data protection in the Union, there is no need to go beyond it. Instead, the alignment will ensure full consistency with the EU personal data protection rules, including those contained in the LED. In this manner, effect is given to the Commission's commitment contained in a 2020 Communication to "*make a legislative proposal, which as a minimum will entail an amendment of Council Framework Decision 2006/960/JHA to ensure the necessary data protection alignment, in the last quarter of 2021*"[40].

4. BUDGETARY IMPLICATIONS

While highly depending from the specificities of each national IT set-up and legal parameters, an estimation of possible costs has been provided by Europol and reported in the Impact Assessment accompanying this proposal. The necessary IT upgrades in both Single Points of Contact and Police and Customs Cooperation Centres[41] were estimated to amount to a maximum **one-off total** of **EUR 11,5 million.** These are deemed to be divided as follows:

– 1,5 million to set-up Case Management Systems (CMS) in 10 MS (not yet equipped);

– 1 million to integrate SIENA in the CMS of the Single Points of Contacts of 20 MS (not yet equipped);

– 2,25 million to establish connection of Police and Customs Cooperation Centres with SIENA in a maximum of 45 Police and Customs Cooperation Centres (14 out of 59 are already connected);

– 6,75 million to set-up CMSs in a maximum of 45 Police and Customs Cooperation Centres (45x EUR 150.000).

These costs (one-off investment) are deemed acceptable and **proportionate** to the identified problem and do not go beyond what is necessary to achieve the specific objectives set out by this proposal for a Directive. It should be noted that Member States are in any case pursuing a modernisation of their IT systems (also in the context of the interoperability of EU information systems). This provides a good opportunity for cost effective implementation of the changes envisaged by the provision of this proposal. These estimations do not cover training needs since, especially for IT upgrades, the training costs are highly depending from the specificities of each national IT set-up and legal parameters.

In any event, the costs at national level should be covered by Member States' programmes under the Internal Security Fund[42]. The Internal Security Fund includes the specific objective to "*improve and facilitate the exchange of information*" and to "*improve and intensify cross-border cooperation*"[43]. When preparing their national programmes, Member States are thus

39 Directive (EU) 2016/680, OJ L 119, 4.5.2016.

40 COM(2020)262, *Way forward on aligning the former third pillar acquis with data protection rules.*

41 Police and Customs Cooperation Centres are regional information hubs set up in border regions of two or more Member States. They are composed by personnel of law enforcement authorities from these Member States. So far, 59 Police and Customs Cooperation Centres have been set up across Europe.

42 Regulation (EU) 2021/1149.

43 See Articles 3(2)(a) and (b) of Regulation (EU) 2021/1149.

invited to include activities relevant for the implementation of the envisaged Directive, with explicit reference to Single Points of Contact and Police and Customs Cooperation Centres, and the connection to SIENA. As some Member States are more advanced than others in their level of cooperation, the cost of implementing the proposed Directive will vary between Member States.

Apart from the costs potentially covered by Member States' programmes under the Internal Security Fund, there will be no other costs borne at EU level.

5. OTHER ELEMENTS

• Implementation plans and monitoring, evaluation and reporting arrangements

The evaluation of impacts of the proposed measures depends on the information to be received from the Member States. For this reason, the present proposal contains **provisions on collection of data indicators**. The responsibility for the collection of the relevant monitoring data should be in the remit of national authorities, ideally the Single Points of Contact. Subsequently, the monitoring of these activity indicators will be used to inform on the application of the proposed measures.

In this connection, the present proposal requires the Commission to submit a report to the European Parliament and to the Council, assessing the extent to which the Member States have taken the necessary measures to comply with this proposed Directive. The relevant article also requires the Commission to submit a report to the European Parliament and to the Council assessing the added value of the Directive, 5 years after the entry into force, and consider a possible review of the Directive upon relevance.

Aside from this legal proposal, the Commission, acting by virtue of its administrative autonomy, will set up an **informal expert group** composed of experts from each Member State, to advise and support the Commission in the monitoring and application of the Directive, including in the preparation of Commission guidance papers. This expert group could be built upon the existing informal Head of the Single Points of Contact' network. Last but not least, the evaluation and monitoring mechanism to verify the application of the Schengen acquis in the field of police cooperation will continue to be carried out, in line with the current Council Regulation[44], and eventually in line with its possible amendment[45]. These evaluation reports have so far covered the implementation of the Swedish Framework Decision. Future evaluations will encompass the application of the envisaged new Directive.

• Detailed explanation of the specific provisions of the proposal

This legislative proposal for a Directive is structured in six chapters:

(1) General provisions for information exchange between Member States' law enforcement authorities for the purpose of preventing, detecting and investigating criminal offences (Art. 1 to Art. 3)

The first block of provisions builds on the structure and substance of the Swedish Framework Decision in force since 2006. In addition, it brings its scope and contents in line with the provisions concerning police cooperation (Title V, Chapter 4) as introduced by the Treaty of Lisbon in force since 2009.

---

44 OJ L 295, 6.11.2013, p. 27–37.

45 Commission proposal for a Council regulation on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing Regulation (EU) 1053/2013, 2 June 2021.

Article 1 defines the scope of application of the horizontal rules for exchanging information for the purposes of preventing, detecting or investigating criminal offences. The provisions of this Directive apply unless otherwise regulated by other, specific acts of EU law.

Article 2 defines a number of key terms, such as the authorities subject to the horizontal rules on information exchange, the criminal offences concerned and the type of information available to law enforcement authorities.

Article 3 outlines three principles that must be respected when exchanging information between the Member States under the Directive: the principle of equivalent access establishing that substantially the same conditions must exist for information exchanges within a Member State and between Member States; the principle of availability stating that if information is available concerning a criminal offence in a Member State, this must, as a general rule, be made available to other Member States as well; and the principle of confidentiality guaranteeing that Member States respect each other's confidentiality requirements when treating such information by ensuring a similar level of protection.

(2) Exchange of information through the Single Point of Contact (Art. 4 to Art. 6)

Article 4 sets out a number of requirements regarding requests for information sent to the Single Point of Contact. This notably concerns criteria justifying the request and qualifying urgency. The request is to be submitted by the Single Point of Contact of other Member States or, where a Member State decides so, by other law enforcement authorities. The language used for the request must be chosen among a list of languages that each Member States is obliged to establish and that is to be published in the Official Journal of the EU.

Article 5 establishes the obligation for the Single Point of Contact receiving the requests for information referred to in Article 4 to process and respond to the requests within precise time limits, which may be derogated from only in certain narrowly specified circumstances, namely, when a judicial authorisation is required. Such provision of information will have to be done in the same language used for the request.

Article 6 lays down an exhaustive list of grounds that the Single Point of Contact may invoke, where objectively justified, to refuse the disclosure of the requested information, of which the relevant authority of the requesting Member State must be promptly informed. The possibility for the Single Point of Contact to seek clarifications as to the content of the requests is foreseen, which will suspend the applicable time limits, yet only if the clarifications are objectively necessary to avoid the request being refused. In respect of other clarifications that may be deemed necessary, there will be no such suspension.

(3) Other exchanges of information (Art. 7 to Art. 8)

Article 7 establishes the obligation for Member States to share information with another (other) Member State(s) spontaneously, i.e. on the relevant authority's own initiative without a request for information having been submitted, when that information is likely to assist in achieving one of the purposes specified in the Directive.

Article 8 ensures that the relevant Single Points of Contact are kept informed of any exchange of information upon request, other than requests submitted to the Single Point of Contact, i.e. either information exchanges upon request handled directly between law enforcement authorities of different Member States or upon requests for information submitted by a Single Point of Contact to a law enforcement authority of another Member State. This includes relevant information exchanges by Police and Customs Cooperation Centres and any other equivalent bodies, in as far as they qualify as law enforcement authorities under the proposed Directive.

(4) Additional rules on the provision of information under Chapter II and III (Art. 9 to Art. 13)

Article 9 addresses situations where, under the national law of the Member State to which relevant information is available, a judicial authorisation is required for the provision of that information, either upon request or spontaneously and either by the Single Point of Contact or by a law enforcement authority. This provision gives effect to and further specifies the principle of equivalent access, meaning that substantially the same conditions must apply when the requested information is subject to judicial authorisation, regardless of the fact that the information is to be provided to an authority of another Member State rather than to an authority of the same Member State. This article also establishes that the authority concerned must immediately take all necessary steps, both practically and legally, in accordance with their national law, to obtain such judicial authorisation as soon as possible.

Article 10 sets out certain requirements aimed at ensuring adequate protection of personal data, resulting in particular from the alignment with the rules of the LED.

Article 11 regulates the language to be used by Single Points of Contact and law enforcement authorities in the situations specified in this Directive, both as regards the actual provision of information and any other communications related thereto. No such language requirements apply to the direct information exchanges and other communications referred to in Article 8. Member States are to establish a list of languages acceptable to them, which should also include English. Such lists must be published by the Commission in the Official Journal of the EU.

Article 12 introduces the obligation for the Single Point Contact as well as all other law enforcement authorities to systematically keep informed Europol (meaning 'put in copy'), insofar as the exchanges concern crimes falling under the scope of Europol's mandate as specified in its basic act. This obligation ensures that Europol can fulfil its role of information hub in the EU in relation to information relevant for law enforcement purposes.

Article 13 requires all relevant authorities to use – and, to that aim, be directly connected to – the Secure Information Exchange Network Application (SIENA), managed by Europol, for all exchanges of information and related communications covered by the Directive. These rules on the mandatory use of SIENA do not apply where specific acts of Union law contain different requirements on the communication channel to be used, for instance for information exchanges governed by the SIS Regulation[46], given that exchanges under such specific acts are excluded from the scope of this Directive.

(5) Minimum requirements on establishing a Single Point of Contact as a central entity to coordinate information exchange between Member States (Art. 14 to Art. 16)

The fifth block of provisions sets out and builds on the obligation for each Member State to establish or designate a Single Point of Contact as the central entity coordinating information exchanges between its law enforcement authorities and those of other Member States within

[46] OJ L 312, 7.12.2018, p. 1–13. Regulation 2018/1860 on the use of the Schengen Information System for the return of illegally staying third-country nationals; Regulation 2018/1861 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation No 1987/2006; Regulation 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation No 1986/2006 and Commission Decision 2010/261/EU, as amended.

the scope of the Directive. It lays out a number of minimum requirements that any Single Point of Contact must comply with.

Article 14 sets out the tasks and capabilities of the Single Point of Contact. In order to carry out its functions, the Single Point of Contact is to have access to the necessary information and be kept systematically informed of all direct information exchanges between its national authorities and those of the other Member States. The actual establishment or designation of the Single Points of Contact must be notified, within a set time period, to the Commission, which must then publish such notifications in the Official Journal of the EU.

Article 15 establishes minimum requirements regarding the composition of the Single Point of Contact, leaving a degree of flexibility to each Member State to determine its precise organisation and composition as deemed most appropriate depending on its national circumstances, provided the requirements of the Directive are met.

Article 16 defines minimum requirements for the Case Management System of the Single Points of Contact.

(6) Final provisions

The final provisions ensure that the implementation of the proposed Directive is properly monitored. Firstly, by the Member States, through the obligation to collect and provide a minimum set of statistical data on a yearly basis (Article 17). Secondly, by the Commission, through the obligation to report to the European Parliament and the Council, having regard inter alia to the data provided by Member States, thus allowing, thirdly, those two institutions to monitor the Directive's implementation as well (Article 18).

Finally, Articles 19, 20, 21, 22 and 23 deal with a number of necessary legal-technical issues, namely, the deletion or repeal of pre-existing rules which the rules of the proposed Directive replace, transposition into national law, as well as entry into force and addressees. As regards the existing rules contained in the CISA (Article 19), Article 39 thereof is replaced only insofar as it relates to information exchange for the purpose specified in the proposed Directive. Article 39 continues to be applicable to other forms of police cooperation covered by that article. In contrast, Article 46 of the CISA, which specifically relates to such information exchange, is fully superseded by the proposed Directive and is therefore deleted.

2021/0411 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Acting in accordance with the ordinary legislative procedure,

Whereas:

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

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

(3) Exchange of information between Member States for the purposes of preventing and detecting criminal offences is regulated by the Convention Implementing the Schengen Agreement of 14 June 1985[47], adopted on 19 June 1990, notably in its Articles 39 and 46. Council Framework Decision 2006/960/JHA[48] partially replaced

[47] 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).

[48] 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).

those provisions and introduced new rules for the exchange of information and intelligence between Member States' law enforcement authorities.

(4) Evaluations, including those carried under Council Regulation (EU) 1053/2013[49], indicated that Framework Decision 2006/960/JHA is not sufficiently clear and does not ensure adequate and rapid exchange of relevant information between Member States. Evaluations also indicated that that Framework Decision is scarcely used in practice, in part due to the lack of clarity experienced in practice between the scope of the Convention Implementing the Schengen Agreement and of that Framework Decision.

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

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

(7) It is necessary to lay down rules governing the cross-cutting aspects of such information exchange between Member States. The rules of this Directive should not affect the application of rules of Union law on specific systems or frameworks for such exchanges, such as under Regulations (EU) 2018/1860[50], (EU) 2018/1861[51], (EU) 2018/1862[52], and (EU) 2016/794[53] of the European Parliament and of the

---

49 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).

50 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).

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

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

53 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).

Council, Directives (EU) 2016/681[54] and 2019/1153[55] of the European Parliament and of the Council, and Council Decisions 2008/615/JHA[56] and 2008/616/JHA[57].

(8) This Directive does not govern the provision and use of information as evidence in judicial proceedings. In particular, it should not be understood as establishing a right to use the information provided under this Directive as evidence and, consequently, it leaves unaffected any requirement provided for in the applicable law to obtain the consent from the Member State providing the information for such use. This Directive leaves acts of Union law on evidence, such as Regulation (EU) …/…[58] [*on European Production and Preservation Orders for electronic evidence in criminal matters*] and Directive (EU) …/…[59] [*laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*], unaffected.

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

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

---

54 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).

55 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).

56 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).

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

58 Regulation proposal, COM/2018/225 final - 2018/0108 (COD).

59 Directive proposal, COM/2018/226 final - 2018/0107 (COD).

they are to be considered as urgent and which explanations they are to contain as minimum.

(11) Whilst the Single Points of Contact of each Member State should in any event have the possibility to submit requests for information to the Single Point of Contact of another Member State, in the interest of flexibility, Member States should be allowed to decide that, in addition, their law enforcement authorities may also submit such requests. In order for Single Points of Contact to be able to perform their coordinating functions under this Directive, it is however necessary that, where a Member State takes such a decision, its Single Point of Contact is made aware of all such outgoing requests, as well as of any communications relating thereto, by always being put in copy.

(12) Time limits are necessary to ensure rapid processing of requests for information submitted to a Single Point of Contact. Such time limits should be clear and proportionate and take into account whether the request for information is urgent and whether a prior judicial authorisation is required. In order to ensure compliance with the applicable time limits whilst nonetheless allowing for a degree of flexibility where objectively justified, it is necessary to allow, on an exceptional basis, for deviations only where, and in as far as, the competent judicial authority of the requested Member State needs additional time to decide on granting the necessary judicial authorisation. Such a need could arise, for example, because of the broad scope or the complexity of the matters raised by the request for information.

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

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

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

(16) It is particularly important that the protection of personal data, in accordance with Union law, is ensured in connection to all exchanges of information under this Directive. To that aim, the rules of this Directive should be aligned with Directive (EU) 2016/680 of the European Parliament and of the Council[60]. In particular, it should be specified that any personal data exchanged by Single Points of Contacts and law enforcement authorities is to remain limited to the categories of data listed in Section B point 2, of Annex II to Regulation (EU) 2016/794 of the European Parliament and of the Council[61]. Furthermore, as far as possible, any such personal data should be distinguished according to their degree of accuracy and reliability, whereby facts should be distinguished from personal assessments, in order to ensure both the protection of individuals and the quality and reliability of the information exchanged. If it appears that the personal data are incorrect, they should be rectified or erased without delay. Such rectification or erasure, as well as any other processing of personal data in connection to the activities under this Directive, should be carried out in compliance with the applicable rules of Union law, in particular Directive (EU) 2016/680 and Regulation (EU) 2016/679 of the European Parliament and of the Council[62], which rules this Directive leaves unaffected.

(17) In order to allow for adequate and rapid provision of information by Single Points of Contact, either upon request or on their own initiative, it is important that the relevant officials of the Member States concerned understand each other. Language barriers often hamper the cross-border exchange of information. For this reason, rules should be established on the use of languages in which requests for information submitted to the Single Points of Contact, the information to be provided by Single Points of Contact as well as any other communications relating thereto, such as on refusals and clarifications, are to be provided. Those rules should strike a balance between, on the

---

60 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).

61 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).

62 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119 4.5.2016, p. 1).

one hand, respecting the linguistic diversity within the Union and keeping costs of translation as limited as possible and, on the other hand, operational needs associated with adequate and rapid exchanges of information across borders. Therefore, Member States should establish a list containing one or more official languages of the Union of their choice, but containing also one language that is broadly understood and used in practice, namely, English.

(18) The further development of the European Union Agency for Law Enforcement Cooperation (Europol) as the Union's criminal information hub is a priority. That is why, when information or any related communications are exchanged, irrespective of whether that is done pursuant to a request for information submitted to a Single Point of Contact or law enforcement authority, or on their own-imitative, a copy should be sent to Europol, however only insofar as it concerns offences falling within the scope of the objectives of Europol. In practice, this can be done through the ticking by default of the corresponding SIENA box.

(19) The proliferation of communication channels used for the transmission of law enforcement information between Member States and of communications relating thereto should be remedied, as it hinders the adequate and rapid exchange of such information. Therefore, the use of the secure information exchange network application called SIENA, managed by Europol in accordance with Regulation (EU) 2016/794, should be made mandatory for all such transmissions and communications under this Directive, including the sending of requests for information submitted to Single Points of Contact and directly to law enforcement authorities, the provision of information upon such requests and on their own initiative, communications on refusals and clarifications, as well as copies to Single Points of Contact and Europol. To that aim, all Single Points of Contact, as well as all law enforcement authorities that may be involved in such exchanges, should be directly connected to SIENA. In this regard, a transition period should be provided for, however, in order to allow for the full roll-out of SIENA.

(20) In order to simplify, facilitate and better manage information flows, Member States should each establish or designate one Single Point of Contact competent for coordinating information exchanges under this Directive. The Single Points of Contact should, in particular, contribute to mitigating the fragmentation of the law enforcement authorities' landscape, specifically in relation to information flows, in response to the growing need to jointly tackle cross-border crime, such as drug trafficking and terrorism. For the Single Points of Contact to be able to effectively fulfil their coordinating functions in respect of the cross-border exchange of information for law enforcement purposes under this Directive, they should be assigned a number of specific, minimum tasks and also have certain minimum capabilities.

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

ensuring the physical presence or the functional availability of such judicial authorities, either within the premises of the Single Point of Contact or directly available on call.

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

(23) The deployment and operation of an electronic single Case Management System having certain minimum functions and capabilities by the Single Points of Contact is necessary to allow them to carry out their tasks under this Directive in an effective and efficient manner, in particular as regards information management.

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

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

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

(27) This Directive constitutes a development of the provisions of the Schengen *acquis* in which Ireland takes part, in accordance with Council Decision 2002/192/EC[63]; Ireland is therefore taking part in the adoption of this Directive and is bound by it.

(28) As regards Iceland and Norway, this Directive constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis*[64] which fall within the area referred to in Article 1, point H of Council Decision 1999/437/EC[65].

(29) As regards Switzerland, this Directive constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[66] which fall within the area referred to in Article 1, point H of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC[67] and with Article 3 of Council Decision 2008/149/JHA[68].

(30) As regards Liechtenstein, this Directive constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[69] which fall within the area referred to in Article 1, point H of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU[70] and with Article 3 of Council Decision 2011/349/EU[71],

---

63 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).

64 OJ L 176, 10.7.1999, p. 36.

65 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).

66 OJ L 53, 27.2.2008, p. 52.

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

68 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).

69 OJ L 160, 18.6.2011, p. 21.

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

71 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

HAVE ADOPTED THIS DIRECTIVE:

Chapter I

General provisions

Article 1
Subject matter and scope

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

   In particular, this Directive establishes rules on:

   (a) requests for information submitted to the Single Points of Contact established or designated by the Member States, in particular on the content of such requests, mandatory time limits for providing the requested information, reasons for refusals of such requests and the channel of communication to be used in connection to such requests;

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

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

   (d) the establishment, tasks, composition and capabilities of the Single Point of Contact, including on the deployment of a single electronic Case Management System for the fulfilment of its tasks.

2. This Directive shall not apply to exchanges of information between the law enforcement authorities of the Member States for the purpose of preventing, detecting or investigating criminal offences that are specifically regulated by other acts of Union law.

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

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

   (b) store information for the purpose referred to in point (a);

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

---

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).

4. This Directive does not establish any right to use the information provided in accordance with this Directive as evidence in judicial proceedings.

Article 2
Definitions

For the purpose of this Directive:

(1) 'law enforcement authority' means any authority of the Member States competent under national law for the purpose of preventing, detecting or investigating criminal offences;

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

(a) offences referred to in Article 2(2) of Council Framework Decision 2002/584/JHA[72];

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

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

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

(4) 'available' information means information that is either held by the Single Point of Contact or the law enforcement authorities of the requested Member State, or information that those Single Points of Contact or those law enforcement authorities can obtain from other public authorities or from private parties established in that Member State without coercive measures;

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

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

Article 3
Principles of information exchange

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

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

(b) the conditions for requesting information from the Single Point of Contact or the law enforcement authorities of other Member States, and those for providing information to the Single Points of Contact and the law enforcement authorities of other Member States, are equivalent to those applicable for

[72] 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).

requesting and providing similar information from and to their own law enforcement authorities ('principle of equivalent access');

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

Chapter II

Exchanges of information through Single Points of Contact

Article 4
Requests for information to the Single Point of Contact

1. Member States shall ensure that their Single Point of Contact and, where they have so decided, their law enforcement authorities submit requests for information to the Single Points of Contact of other Member States in accordance with the conditions set out in paragraphs 2 to 5.

   Where a Member State has decided that, in addition to its Single Point of Contact, its law enforcement authorities may also submit requests for information to the Single Points of Contact of other Member States, it shall ensure that those authorities send, at the same time as submitting such requests, a copy of those requests, and of any other communication relating thereto, to the Single Point of Contact of that Member State.

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

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

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

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

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

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

   (b) necessary in order to protect a person's vital interests which are at imminent risk;

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

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

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

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

(b) a description of the purpose for which the information is requested;

(c) the objective reasons according to which it is believed that the requested information is available to the law enforcement authorities of the requested Member State;

(d) an explanation of the connection between the purpose and the person or persons to whom the information relates, where applicable;

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

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

Article 5

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

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

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

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

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

The time periods laid down in the first subparagraph shall commence at the moment of the reception of the request for information.

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

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

(i) immediately inform the Single Point of Contact or, where applicable, the law enforcement authority of the requesting Member State of the expected delay, specifying the length of the expected delay and the reasons therefore;

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

3. Member States shall ensure that their Single Point of Contact provides the information requested in accordance with Article 4 to the Single Point of Contact or, where applicable, the law enforcement authority of the requesting Member State, in the language in which that request for information was submitted in accordance with Article 4(5).

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

Article 6

Refusals of requests for information

1. Member States shall ensure that their Single Point of Contact only refuses to provide the information requested in accordance with Article 4 insofar as any of the following reasons applies:

   (a) the requested information is not available to the Single Point of Contact and the law enforcement authorities of the requested Member State;

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

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

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

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

      (i) be contrary to the essential interests of the security of the requested Member State;

      (ii) jeopardise the success of an ongoing investigation of a criminal offence; or;

      (iii) unduly harm the vital interests of a natural or legal person.

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

2. Member States shall ensure that their Single Point of Contact informs the Single Point of Contact or, where applicable, the law enforcement authority of the requesting Member State of the refusal, specifying the reasons for the refusal, within the time limits provided for in Article 5(1).

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

   The time limits referred to in Article 5(1) shall be suspended from the moment that the Single Point of Contact or, where applicable, the law enforcement authority of the requesting Member State receives the request for clarifications, until the moment

that the Single Point of Contact of the requested Member State receives the clarifications.

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

Chapter III

Other exchanges of information

Article 7
Own-initiative provision of information

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

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

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

Article 8
Exchanges of information upon requests submitted directly to law enforcement authorities

Member States shall ensure that, where Single Points of Contact or law enforcement authorities submit requests for information directly to the law enforcement authorities of another Member State, their Single Points of Contact or their law enforcement authorities send, at the same time as they send such requests, provide information pursuant to such requests or send any other communications relating thereto, a copy thereof to the Single Point of Contact of that other Member State and, where the sender is a law enforcement authority, also to the Single Point of Contact of its own Member State.

Chapter IV

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

Article 9
Judicial authorisation

1. Member States shall not require any judicial authorisation for the provision of information to the Single Points of Contact or law enforcement authority of another Member State under Chapters II and III, where no such requirement applies in respect of similar provision of information to their own Single Point of Contact or their own law enforcement authorities.

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

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

Article 10

Additional rules for information constituting personal data

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

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

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

Article 11

List of languages

1. Member States shall establish and keep up to date a list with one or more of the official languages of the Union in which their Single Point of Contact is able to provide information upon a request for information or on its own initiative. That list shall include English.

2. Member States shall provide those lists, as well as any updates thereof, to the Commission. The Commission shall publish those lists, as well as any updates thereof, in the Official Journal of the European Union.

Article 12

Provision of information to Europol

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

Article 13
Use of SIENA

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

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

Chapter V

Single Point of Contact for information exchange between Member States

Article 14
Establishment, tasks and capabilities

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

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

   (a) receive and evaluate requests for information;

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

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

   (d) provide, upon request or upon its own initiative, information to the Single Points of Contact and, where applicable, to the law enforcement authorities of other Member States in accordance with Articles 5 and 7;

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

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

3. Member States shall ensure that:

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

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

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

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

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

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

Article 15
Composition

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

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

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

(b) the SIRENE Bureau established by Article 7(2) of Regulation (EU) 2018/1862 of the European Parliament and of the Council[73];

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

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

Article 16
Case Management System

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

[73] 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).

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

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

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

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

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

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

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

(h) logging of access and of other processing activities in relation to the information contained in the Case Management System, for accountability and cybersecurity purposes.

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

3. Member States shall ensure that any personal data processed by their Single Point of Contact are contained in the Case Management System only for as long as is necessary and proportionate for the purposes for which the personal data are processed and are subsequently irrevocably deleted.

Chapter VI

Final provisions

Article 17
Statistics

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

2. The statistics shall cover, as a minimum:

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

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

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

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

Article 18
Reporting

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

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

Article 19
Amendments to the Convention Implementing the Schengen Agreement

From [*the date referred to in Article 21(1), the first subparagraph*], the Convention Implementing the Schengen Agreement is amended as follows:

   (i) Article 39 is replaced by this Directive insofar as that article relates to the exchange of information for the purpose referred to in Article 1(1) of this Directive;

   (ii) Article 46 is deleted.

Article 20
Repeal

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

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

Article 21

Transposition

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

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

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

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

Article 22

Entry into force

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

Article 23

Addressees

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

Done at Brussels,

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