Council of the European Union

Brussels, 17 December 2024
(OR. en)

17022/24

JAI 1886
MIGR 467
COMIX 518

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	17 December 2024
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2024) 287 final
Subject:	COMMISSION STAFF WORKING DOCUMENT On the return of illegally staying third-country nationals posing a security threat

Delegations will find attached document SWD(2024) 287 final.

Encl.: SWD(2024) 287 final

EUROPEAN
COMMISSION

Brussels, 16.12.2024
SWD(2024) 287 final

COMMISSION STAFF WORKING DOCUMENT

On the return of illegally staying third-country nationals posing a security threat

Returning illegally staying third-country nationals posing a security threat has been a high priority in the context of return policy. The Return Directive[1] provides for the possibility to apply stricter rules for third-country nationals posing a security threat, such as not granting a period for voluntary departure and issuing an entry bans longer than five years.

Recent changes introduced by the legislation of the Pact on Migration and Asylum[2] have further enhanced these measures. Specifically, third-country nationals posing a security threat will be processed through the return border procedure[3]. This procedure includes a separate ground for detaining returnees who pose a security threat, making it easier to detain them[4] compared to the standard rules outlined in the Return Directive.

To support these efforts, the Commission has strengthened coordination between Member States and the EU Return Coordinator has been working closely with them to accelerate the return process, ensuring a more efficient and effective approach to addressing security threats posed by illegally staying third-country nationals.

The return of third-country nationals posing a threat to public policy, to public security or to national security (hereinafter referred to as a 'security threat') continues to be a political priority. Since November 2023, the topic has been addressed in the context of the work of the High-Level Network for Returns (hereafter "High-Level Network"), a group of senior representatives of Member States, Schengen Associated Countries, Frontex and the EU Asylum Agency established by Commission Communication on a New Pact on Migration and Asylum.

Beyond recurring return-related challenges[5], the network identified specific issues, which are connected to:

- **sharing information on the illegally staying third-country national posing a threat to public policy, public security or to national security**, and;
- **managing and prioritising such return cases**.

This practical, informal and non-binding Commission Staff Working Document was drawn up by Commission services and specifically the EU Return Coordinator, based on exchanges in the High-Level Network on Member States practices and challenges. It is addressed to migration management authorities and aims at **closing information gaps and further ensuring an effective approach** to managing the return of illegally-staying third-country nationals posing a security threat. This document provides an overview of the existing legislative acquis and Member States' current practices in order to make full use of all existing tools to swiftly return third-country nationals posing a security threat.

The Return Directive provides for various provisions regarding third-country nationals posing a security threat:

[1] Directive 2008/115/EC.
[2] Commission Communication of 23.9.2020 - COM(2020) 609 final.
[3] Regulation (EU) 2024/1349 of 14 May 2024 establishing a return border procedure.
[4] Article 5 (3) *ibid*.
[5] Such as the identification and issuing of travel documents, absconding due to limited detention capacity, and the abuse of asylum system through repetitive unfounded asylum claims.

- the possibility to shorten or refrain from granting a period for voluntary departure (Article 7(4));
- the issuance of a return decision to a person posing a security threat who holds a residence permit issued by another Member State (Article 6(2));
- in case of serious threat to public policy, public security or national security, the possibility to issue an entry ban of more than 5 years (Articles 11 (2) and 11(3)).

Importantly, Member States may also choose **not to apply the provisions of the Return Directive** to third-country nationals who are subject to return as a criminal law sanction or as a consequence of a criminal law sanction, according to national law, or who are the subject of extradition procedures (Article 2(2)(b).

Those Member States must nonetheless respect **the principle of non-refoulement** which is a fundamental right under Article 19 of the Charter of Fundamental rights.

Specific attention shall be given to the guarantees included in the Directive for children (including unaccompanied) for all steps of the return procedure.

The first part of this document focuses on sharing information and carrying out a **security check** related to establishing whether the illegally staying third-country national to whom a return decision is issued, poses a threat to public policy, public security, or to national security**.** The document aims at laying out the elements that can be considered forming part of **minimum standards for such security check on returnees.** Since March 2023 with the entry into operation of the renewed Schengen Information System (SIS)[6], when entering into SIS alerts on third-country nationals subject to a return decision, Member States have the possibility to share data in the alerts on those third-country nationals that pose a threat to public policy, public security or to national security.

The second part of the document looks at **the case management of third-country nationals** subject to a return decision and posing a security threat in relation to whom particular attention is needed to initiate and follow-up the return procedure diligently, also to ensure that the third-country national does not abscond. In practice most Member States **prioritise such cases** and manage them separately from the regular return case flow in cooperation with law enforcement and/or other national security actors.

The third part of the document highlights **Member States' good practices** managing returns with a security aspect.

1. SHARING INFORMATION ON ILLEGALLY STAYING THIRD-COUNTRY NATIONALS POSING A SECURITY THREAT

Since March 2023, Member States are required to enter a return alert in the SIS on third-country nationals subject to return decisions, without delay following the issuance of a return decision[7]. The return alert does not only contain personal data of the third-country national, but also

[6] Regulation (EU) 2018/1860 of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals.
[7] Article 3 of Regulation 2018/1860.

information on '*whether the return decision is issued in relation to a third-country national who poses a threat to public policy, to public security or to national security*'[8], the so-called 'security flag'. The security check constitutes an integral part of the national return process and is reflected in the national return decision and the corresponding SIS return alert.

1.1 When issuing the return decision and before entering the return alert in the SIS, systematic checks, based on national protocols and/or arrangements with the relevant law enforcement and security actors in the Member State, are necessary **to determine whether a security check has already been carried out.**

1.2 In general, Member States aim at carrying out a security check on third-country nationals as early as possible in any migration procedure. This starts from the visa application procedure for those who need it, or upon arrival at a border crossing point where third-country nationals are also crosschecked against the SIS, Interpol's Stolen and Lost Travel Documents database (SLTD), relevant national databases and EURODAC where relevant. In the near future, certain visa-exempted third-country nationals will undergo some security checks to obtain a travel authorisation before entering the EU, the ETIAS. For those entering the EU irregularly, the security check will be carried out upon entry, in accordance with the new Screening Regulation (Art. 11)[9]. Security underlines the new Asylum and Migration Management Regulation[10]. The security checks are part of the general principles of the new Regulation, they should precede Dublin determination: only when verifying that the person is not a threat to the internal security, the Member State can proceed with the Dublin determination.

The annex to this document provides a list of the access to migration-related information in EU information systems that can be accessed for the purpose of the prevention, detection and investigation of terrorist offences or other serious criminal offences and that can provide valuable information in case a third-country national is subject to a return decision.

1.3 If no security check was carried out early in the migration-related procedure, in several Member States**, the authority issuing the return decision is responsible for carrying out or ensuring that a security check is made by the competent authority** to determine whether the third-country national poses a security threat. Several Member States have in place systematic checks as part of the process to issue a return decision. Most Member States have established **a framework and a national procedure for information exchange** among their own national authorities, and if necessary, complemented with guidelines and protocols for information sharing.

The security check can be designed in a way that **it does not slow down the implementation of effective return.**

[8] Article 4(1)(o) of Regulation 2018/1860.
[9] Regulation of the European Parliament and of the Council (EU) 2024/1356 introducing a screening of third-country nationals at the external borders and amending Regulations (EC) 767/2008, (EU) 2017/2226, (EU) 2018/1240, and (EU) 2019/817.
[10] Article 8(4) of Regulation (EU)2024/1351 of the European Parliament and of the Council of 14 May 2024 on asylum and migration management, amending Regulations (EU) 2021/1147 and (EU) 2021/1060 and repealing Regulation (EU) 604/2013.

In the counter-terrorism domain, Member States have developed a "shared understanding"[11] on when a person could be regarded as a potential terrorist or violent extremist threat to facilitate sharing of information on such individuals through EU information systems. This "shared understanding" does not constitute a formal definition. The criteria on when a person should be regarded as a potential terrorist or violent extremist threat are strictly non-binding, do not affect the existing mechanisms and procedures already established at European and national level. The criteria serve to promote the inclusion of such individuals into the European databases and information systems by the Member States subject to the legal requirements governing these systems. Based on these criteria, it is highly likely that these individuals are already included in EU databases and would be identified during the check in those databases.

1.4 **The following databases** are central for the purpose of the security check:

- SIS, in accordance with the provisions of Article 34 of Regulation (EU) 2018/1861[12] and Article 44 of Regulation (EU) 2018/1862[13].
- National databases of the Member State responsible for carrying out the assessment of the threat, including national criminal records if access is allowed in accordance with national law.

In case there are grounds to consider that the person is a potential security threat, additional checks may be needed. The consultation of additional databases requires cooperation between the return authorities and the relevant authorities that are competent in accessing these databases. The following additional databases are key in such cases:

- Databases maintained by national law enforcement authorities in other Member States through established EU law enforcement cooperation channels[14]. These channels, most notably the national Single Point of Contact (SPOC), allow for the exchange of identity-related details to support cross-border law enforcement cooperation.
- National criminal dactyloscopic databases of other Member States via automated searches under the Prüm framework[15] for the purpose of the prevention, detection, and investigation of crime offences, on the basis of fingerprints (dactyloscopic data) when collection and use of such data is allowed under national law,

[11] Council document 9988/24.
[12] OJ 07.12.2018, L 312, p. 14.
[13] OJ 07.12.2018, L 312, p. 56.
[14] Member States must implement the Directive 2023/977 on the exchange of information between the law enforcement authorities of Member States by 12 December 2024.
[15] Council Decisions 2008/615/JHA and 2008/616/JHA as well as the Prüm II Regulation (EU) 2024/982 which will repeal the provisions on automated exchanges of the previous Council Decision. The Prüm Regulation is a framework to exchange valuable data in an automated manner between authorities responsible for the prevention, detection and investigation of criminal offences. The Prüm Regulation allows identifying a person using biometric samples (DNA profiles and dactyloscopic data) found on a crime scene, or from a license plate or vehicle registration number discovered during a criminal investigation. Member States can identify a person through their national biometric databases. The Prüm Regulation allows to do it also using other Member States' databases, which is very important in an area without internal borders.

- Future centralised European Criminal records Information System on non-EU criminals (ECRIS-TNC)[16] and national criminal records of other Member States when access is allowed under national law,
- Europol Information System (EIS)[17], and
- Interpol databases, provided that searches are carried out by competent law enforcement authorities.

1.5 If the returnee poses a security threat, a **'security flag'**, in the meaning of Art. 4 (1), point (o) of Regulation (EU) 2018/1860, must be inserted in the SIS return alert. If new elements emerge during the return procedure, the return alert can be updated at a later stage.

1.6 **Besides adding the 'security flag' in the return alert, the authority must enter all available data relevant to the alert[18] into the SIS, including:**

- information needed **to identify the person**, including all known aliases (name/surname/date of birth/previously used names and aliases/place of birth/nationalities held),
- warning markers about the person, e.g. whether the person is armed, violent or **has absconded** or escaped, is involved in an activity referred to in Articles 3 to 14 of Directive (EU) 2017/541 on combating terrorism,
- photographs of the person,
- 'dactyloscopic data' (fingerprints, palm prints) of the person,
- 'type of offence' committed by the person, if applicable, and
- 'identification document descriptions'[19],
- a copy of the identification documents.

It is important that all available data, is included in the SIS, while ensuring the highest possible level of data quality. **Warning markers** play a crucial role in warning the Member State's authorities dealing with the third-country nationals in person about the nature of the risks or special circumstances they may face.

In relation to third-country nationals posing a security threat who temporarily cannot be removed due to the risk of violating the principle of non-refoulement, Member States can consider whether to issue **a different category of alert in the SIS, such as a**

[16] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised ECRIS-TCN system and amending Regulation (EU) 2018/1726.
[17] It is Europol's central criminal information and intelligence database, which covers all of Europol's mandated crime areas.
[18] Art.4 of Regulation (EU) 2018/1860.
[19] This refers to the following data categories of Article 4 of Regulation (EU) 2018/1860: (q) the category of the person's identification documents; (r) the country of issue of the person's identification documents; (s) the number(s) of the person's identification documents; (t) the date of issue of the person's identification documents.

discreet check alert[20]. It should be recalled, however, that a Member State can only issue one category of alert on a person of concern[21].

1.7 The national authority can also insert the information that the third-country national poses a security threat, in its own databases and flag these cases as a 'priority'. It is important that this information is available to all relevant authorities.

2. MANAGING AND PRIORITISING RETURN CASES WITH A SECURITY ASPECT

When the returnee poses a security threat, the best practice identified in discussions with Member States is **to prioritise the case management and accelerate the return of the individual**, unless there are security reasons for not doing so and requesting that the returnee remain on the territory. **Managing the cases separately from the regular return case flow and in cooperation with law enforcement and/or other national security actors ensures close follow-up.** Member States' good practices included at the end of this document serve as a source of inspiration in this respect, including in the following areas:

2.1 The **risk of absconding** should be assessed carefully at the beginning of the return process, and the necessary measures are taken including detention for the purpose of removal or detention based on another national ground. Certain Member States monitor constantly the risk of absconding and keep available the necessary detention capacity.

2.2 If the returnee posing a security threat absconds, the return alert should be updated with this information[22] .

2.3 In case of **a hit on a SIS return alert containing a 'security flag'** regarding a third-country national present on the territory of a Member State other than the one which issued the alert, the authorities of the Member State conducting the SIS check, must immediately inform the Member State that issued the return alert[23]. **The 'security flag' must be taken into consideration when determining the follow-up to be given to the SIS hit**, including by mutually recognising the return decision and managing the risk of absconding, to the fullest extent possible under the applicable national law.

In addition, in case of a hit on a SIS return alert (even without a 'security flag'), the Member State must communicate the circumstances of the hit to the Member State that issued the alert via the SIRENE network. The exchange of the relevant information should take place as soon as possible. Member States may also request any necessary supplementary information on a SIS alert.

[20] In Regulation (EU) 2018/1862, each SIS alert on a person is issued for a specific purpose: Article 26 applies when the person is wanted with a European Arrest Warrant or for extradition purposes; Article 32 applies for missing persons or vulnerable persons to be prevented from traveling; Article 34 applies for persons sought to assist with a judicial procedure; Article 36 is used for discreet checks, inquiry checks or specific checks may be entered for the purposes of preventing, detecting, investigating or prosecuting criminal offences, executing a criminal sentence and preventing threats to public security; Article 37a is issued based on information provided by third-country authorities and international organisations to Europol on third-country nationals in the interest of the Union.

[21] One of the guiding principles of the SIS is that only one SIS alert per person per Member State can be entered, meaning that if the return alert is already in the SIS, the Member State that issued it cannot add any other alert on the same person, unless the return alert is deleted and another one introduced.

[22] Art.4 of the Regulation (EU) 2018/1860

[23] Art.7(2) *ibid*.

Further possible steps:

- request to national law enforcement databases of other Member States via EU law enforcement cooperation channels[24], most notably via the national Single Point of Contact (SPOC), based on identity details;

- request to national criminal dactyloscopic databases of other Member States via automated searches under the Prüm framework[25] for the purpose of the prevention, detection and investigation of criminal offences, on the basis of fingerprints (dactyloscopic data) when collection and use of such data is allowed under national law;

- exchange information with the relevant national authorities, including national security services i.e. through the Central Contact Point appointed for the exchange of unclassified administrative information between migration/asylum authorities and counter-terrorism authorities in the Member State. A **compendium on the *'Information exchange between counter-terrorism authorities and immigration and asylum authorities'*** drawn up by the Council lists the Central Contact Points in Member States' migration/asylum authorities to further facilitate international cooperation and information exchange between Member States.

  The communication channels between intra-EU homologous services are the privileged channel chosen by the compendium. In this case, exchange of information takes place between the security services of the two or more Member States involved and is transmitted in the agreed form to the migration services.

Migration authorities' mutual support plays an important role in facilitating the identification of the persons concerned, by adding **as much information as possible to the SIS alert or by transmitting supplementary information on request of the other Member State concerning identity or other elements related to return without delay**.

Competent Member States' authorities assess whether the return of the third-country national posing a security threat respects the principle of *non-refoulement* in accordance with the Charter of Fundamental Rights, the Return Directive and the case-law of the Court of Justice of the European Union. Moreover, if the returnee posing a security threat cannot be returned to the country of origin, there is the possibility to be **return him or her to a country of transit or another third country to which the third-country national concerned voluntary decides to return and in which he or she will be accepted[26].**

[24] Directive 2023/977 on the exchange of information between the law enforcement authorities of Member States by 12 December 2024.
[25] *ibid*
[26] Article 3§3 of Return Directive 2008/115/EC.

2.4 Most Member States accompany the return decision with **an entry ban of the maximum possible duration,** and a corresponding alert for refusal of entry and stay is issued in the SIS without delay **once the person has left the EU/Schengen area**.

2.5 When the person to be returned is not in possession of travel documents, most Member States start the readmission procedure without delay with the competent consular authorities, in line with the relevant EU or bilateral Readmission Agreement/Arrangement where relevant. Completeness of the identification/readmission request facilitates this procedure. If no documentation is available, a request for an identification can be submitted to the consular authorities with high priority.

Article 15 of SIS Regulation on return establishes the rules for the "*transfer of personal data to third-countries for the purpose of return*". **Certain data contained in the SIS may be transferred or made available with the agreement of the Member State that entered the return alert** and only where the following conditions are met:

- The data is transferred or made available solely for the purpose of identification of an illegally staying third-country national and issuance of identification or travel document in view of the return of that third-country national.
- The third-country national concerned has been informed that his/her personal data may be shared with the authority of a third country.

Photographs, dactyloscopy data and copies of identity documents are among the data which may be transferred.

2.6 **Frontex offers prioritisation of cases for its charter flights for returnees posing a security threat**; even smaller dedicated charters can be organised with the agreement of the Member State concerned**.**

3. EXAMPLES OF MEMBER STATES' GOOD PRACTICES

3.1 *Joint Task Forces*

Some Member States have established joint special groups/teams/task forces consisting of various stakeholders engaged in the migration process to manage the return of third-country nationals posing a security threat. For instance, a task force can consist of representatives responsible for migration, justice, foreign affairs, return, prison system and national security.

3.2 *Drafting special protocols for handling cases of security threats*

Some Member States have established special protocols for handling individuals posing a security threat throughout the entire migration process. These checklists enable the case-handlers to manage cases involving a third-country national identified as a security threat, consistently and coherently, guiding them through the steps of threat identification, return case management, and ultimately the enforcement of the return decision.

3.3 *Examination in case of diplomatic assurances from a third country*

Some Member States request a diplomatic assurance from the third-country of return as an element that supports the assessment of the respect of the principle of non-

refoulement. In this respect, "*the European Court of Human Right has been called upon to examine whether or not diplomatic assurances by the receiving state can obviate the risk of ill-treatment a person would otherwise be exposed to on return. In cases where the receiving state has provided assurances, those assurances, in themselves, are not sufficient to ensure adequate protection against the risk of ill-treatment. There is an obligation to examine whether or not the practical application of assurances provides a sufficient guarantee that the individual will be protected against the risk of ill-treatment. The weight given to assurances by the receiving state in each case depends on the circumstances prevailing at the material time*."[27]

3.4 ***Dedicated case-manager***

Some Member States designate a dedicated case manager to keep track of the cases of third-country nationals posing a security threat throughout the whole migration process. The case manager also serves as a point of contact for other internal and external actors.

3.5 ***Organising special training***

In some Member States, providing training to personnel is a first step to effectively manage exceptional cases involving third-country nationals who pose a security threat. Among others, the case handler learns how to identify the third-country nationals who might pose a security threat early in the migration process through a series of interviews.

The training should provide case managers with linguistic tools and tools to gather in-depth knowledge of the political, geographical and social context of each country of origin of the third-country nationals to be returned.

3.6 ***Using Information exchange within General Directors of Immigration Services Conference (GDISC)***

The GDISC is an informal network established to facilitate practical cooperation in the field of asylum and migration between the General Directors of Immigration Services of more than 30 European countries, including Member States, but outside the EU framework. This network could also be used to exchange information and good practices even if it should avoid duplicating the work already done at EU level. A GDISC working group is especially dedicated to the facilitation of practical cooperation between migration services on security-related matters. To join the GDISC Security Network, the National Contact Point of a GDISC Member shall notify the GDISC Secretariat and nominate a specific network contact person responsible for security matters.

3.7 ***Creating mobile law enforcement liaison officers (ARLO)***

Good cooperation and communication with third countries tends to result from early relationship-building and personal relationship of trust between the liaison officer and the third-countries authorities. In case long-term deployments are not possible, Member State can set up short-term deployments of mobile police liaison officers to third countries as a flexible solution to handle difficult return cases, as already done by one Member State.

[27] European Agency for Fundamental Rights, "Handbook on European law relating to asylum/borders/immigration".

Such liaison officers could be deployed for short periods of time (e.g. up to three months) to facilitate return and readmission of specific and particularly challenging cases including the return of third-country nationals posing a security threat or those convicted of a crime.

3.8 ***Reduction of the prison sentences in exchange of cooperation to return***

Current practice shows that many Member States have established close cooperation and workflows between the relevant national authorities (e.g. penitentiary authorities and returns authorities) in order to initiate the return procedure with regard to third-country nationals sentenced to prison.

Some Member States have automatic notifications from the penitentiary authorities to the immigration authorities or fixed chains of digital communication between the penitentiary authorities and the local police district responsible for return. The identification and documentation procedures are also mostly initiated prior to release.

In several Member States, return counselling is provided to convicted persons during their prison sentences. If they agree to return to their country of origin on a voluntary basis and are willing to cooperate, half of the sentence can be suspended, and assistance to voluntary return can be provided. Early release from prison is therefore seen as an incentive for effective returns. Careful case management ensures that the return is scheduled for the day of the release.

These examples taken from Member States' practice can be used as a toolbox for tailor-made solutions for the return of illegally staying third-country nationals posing a security threat.

Annex - Access to migration-related information in EU information systems for the purpose of the prevention, detection and investigation of terrorist offences or other serious criminal offences

In order to ensure strict compliance with the conditions for access as established by the relevant EU and national acts, validation is required for individual access by national competent authorities for the purposes of the prevention, detection and investigation of terrorism offences and other serious criminal offences relating to data held in EU information systems, such as the Visa Information System (VIS), Eurodac, the Entry/Exit System (EES), and the European Travel and Information and Authorisation System (ETIAS). The validation is accomplished through ex-ante verification by a separate and independent authority (central access point(s), verifying authority).

1. FUTURE QUERY IN THE COMMON IDENTITY REPOSITORY (CIR)

When the Common Identity Repository (CIR) established under Regulation (EU) 2019/817 and Regulation (EU) 2019/818[28] will become operational, designated authorities will be able to access the CIR under certain conditions. Article 22 of Regulation (EU) 2019/817 and Regulation (EU) 2019/818 (Interoperability Regulations) will make it possible for the Member States' designated authorities and Europol to query the Common Identity Repository (CIR) for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences (so-called first step of the law enforcement access).

When designated authorities launch a query in the CIR in accordance with Article 22 of Regulation (EU) 2019/817, and where the conditions for access laid down in this Article are met, they may request full access to the database where the reply received as referred to in Article 22(2) of that Regulation reveals that data are stored in this database.

The idea behind the CIR query is to enable designated authorities and Europol, before requesting full access to data stored in the system(s) through central access points, to verify whether any of the systems (ETIAS, EES, VIS and Eurodac) contains data on the person concerned.

In reply to the query in the CIR, designated authorities or Europol will receive a 'match' or 'no match' reply. In the case of match(es), designated authorities or Europol will receive a reference(s) to the EU information system(s) that contains data about the person, e.g. match, data can be found in VIS and Eurodac. No other data will be returned. On the basis of this information, designated authorities and Europol can request full access to data stored in the

[28] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of 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 (OJ L 135, 22.5.2019, p. 27) and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).

systems according to the rules laid down in the regulations establishing the underlying systems (so-called second step of the law renforcement access as described above).

2. VISA INFORMATION SYSTEM (VIS)

The Visa Information System (VIS) is a centralised database designed to support the implementation of the Union's visa policy and to strengthen internal security. Its primary purpose is to facilitate the exchange of visa-related data between Member States, enabling effective checks on individuals applying for short-stay visas or crossing the external borders. Additionally, the VIS allows for the identification of persons who may not meet the conditions for entry or stay within the Schengen Area. It also supports the prevention, detection, and investigation of terrorist offenses and serious crimes by granting access to Member States' law enforcement authorities and Europol under strict data protection safeguards.

The authorities designated by the Member States in accordance with Council Decision 2008/633/JHA[29] may consult the VIS if it is necessary appropriate and proportionate to the performance of their tasks and in particular where there are reasonable grounds for believing that such a search would substantially help in preventing, detecting and investigating terrorism offences or other serious criminal offences.

Which authorities can consult the VIS for law enforcement purposes?
National authorities responsible for the prevention, detection and investigation of terrorist offences or other serious criminal offences and designated by the Member States in accordance with Council Decision 2008/633/JHA. Only duly empowered staff of the operational units within the designated authorities can consult and use information from the VIS for law enforcement purposes based on the provisions of Council Decision 2008/633/JHA.

Which data can be searched?
Designated authorities can search with any of the following data:

surname, surname at birth (former surname(s)); first name(s); sex; date of birth, place and country of birth; current nationality and nationality at birth; type and number of the travel document, the issuing authority and the date of issue and of expiry; main destination and duration of the intended stay; purpose of travel; intended date of arrival and departure; intended border of first entry or transit route; residence; fingerprints; type of visa and the number of the visa sticker; details of the person issuing an invitation and/or liable to pay the applicant's subsistence costs during the stay.

Consultation of the VIS will, in the event of a hit, give access to any other data taken from the application form, photographs, the data entered in respect of any visa issued, refused, annulled, revoked, or extended.

[29] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (OJ L 218, 13.8.2008, p. 129).

3. SCHENGEN INFORMATION SYSTEM (SIS)

The SIS enables competent authorities, such as police, border guards, migration and visa authorities to consult alerts on wanted or missing persons and objects.

The SIS is the largest information sharing system for security and border management in Europe. An alert on a person or object entered in SIS by one country becomes available in real time in all the other countries that use the system, so that competent authorities across the Union and the Schengen associated countries can locate the person or object and take the required action. By supporting external border checks and operational cooperation between Member States' competent authorities, the SIS constitutes an essential tool to ensure the free movement of persons while maintaining a high level of security within the Union.

What types of 'migration-related' alerts exist in the SIS?
'Alerts on return' - Article 3 of Regulation (EU) 2018/1860[30]

This alert category concerns illegally staying third-country nationals subject to a return decision, which imposes an obligation to return to their country of origin or another third country. The alert on return in the SIS is issued to verify that the obligation to return has been complied with. Alerts on return include information on whether the return decision is accompanied by an entry ban, and, where relevant, whether the decision is issued in relation to a third-country national who poses a threat to public policy, public security or national security ('security flag').

'Alerts for refusal of entry and stay' - Articles 24 and 25 of Regulation (EU) 2018/1861[31]

This category of alert serves two main purposes:

1) preventing entry into the territory of the Member States and Schengen associated countries for third-country nationals where an entry ban decision has been taken by a Member State that they should not be permitted to enter, notably in accordance with the Return Directive; and

2) ensuring the removal from the territory of the Member States and Schengen associated countries of third-country nationals who are found on that territory but are subject to a decision by a Member State that they should not have entered and have no permission to stay.

Which data can be found in a SIS alert?
A SIS alert contains biometrical data - information required to identify the person, including all known aliases (name/surname/date of birth/previously used names and aliases/place of birth/nationalities held). It might also contain dactyloscopic data – fingerprints and palm prints of the person. The alert also contains case-related data, such as the type of offence and action to be taken. All alert categories may also include warning markers (e.g. that the subject of the alert is armed, violent, or is involved in terrorism-related activity). The authorities can search

[30] 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).
[31] Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 07/12/2018, p. 14).

the SIS based on alphanumeric data (name/surname/date of birth) or solely on the basis of fingerprints or dactyloscopic data.

Which authorities can access data in SIS?
National competent authorities have access to data entered in the SIS for border control, police and customs checks, for examining visa applications and taking decisions related to the entry and stay of third-country nationals. This includes a number of authorities, including national judicial authorities.

The renewed SIS legal framework, applicable since March 2023, has extended the access rights of national authorities. It is explicitly provided that in addition to police checks, national authorities responsible for the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties, within the Member State concerned, provided that Directive (EU) 2016/680 applies, have access to SIS data. Migration authorities have the right to access all types of alerts in SIS.

In addition, Europol and the European Border and Coast Guard teams, teams of staff involved in return-related tasks, and members of the migration management support teams also have access to all SIS alert categories including 'migration-related' alerts.

The detailed list of competent authorities in each Member State authorised to search the "data contained in SIS is maintained by eu-LISA:

https://www.eulisa.europa.eu/Publications/Reports/SIS%20LoA,%20N.SIS,%20SIRENE%202023.pdf

4. EURODAC

Eurodac is the EU's fingerprint database designed to support the implementation of the Dublin Regulation[32]. Its primary objective is to assist Member States in determining the Member State responsible for examining an application for international protection. By enabling the comparison of fingerprint data, Eurodac facilitates the identification of individuals who have previously lodged an application for international protection or who have irregularly crossed the external borders of the Union.

The information contained in Eurodac is also necessary for the purposes of the prevention, detection and investigation of terrorist offences or other serious criminal offences. Therefore, the data in Eurodac is available, subject to the conditions set out in Regulation (EU) 603/2013[33], for comparison by the designated authorities of Member States and Europol. The Eurodac

[32] Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast).
[33] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) (OJ L 180, 29.6.2013, p. 1).

recast Regulation (EU) 2024/1358 is not applicable yet and will start to apply from 12 June 2026.

Which authorities can consult Eurodac for law enforcement purposes?
National authorities which are responsible for the prevention, detection and investigation of terrorist offences or other serious criminal offences and are designated by the Member State to request comparisons with Eurodac data pursuant to Regulation (EU) 603/2013 (current).

Which data can be searched?
Current: Those requests can be carried out only with fingerprint data.

Procedure to consult for law enforcement purposes

Recast: Regulation (EU) 2024/1358 sets out that designated authorities may only access Eurodac if a prior check on national fingerprint databases and criminal dactyloscopic databases of all (if technically possible) other Member States via Prüm has returned a negative result. If there are reasonable grounds that searches via Prüm will not lead to the identification of a person, this check is not necessary. In addition to these prior checks, designated authorities may also conduct a search in the VIS which can be submitted simultaneously with the Eurodac request.

Current Regulation: The abovementioned procedure for access to Eurodac under Regulation (EU) 603/2013 is similar; the negative check in the VIS is mandatory.

Access to Eurodac by Europol
Europol-designated authority may request comparisons with Eurodac data the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences within the limits of Europol's mandate and where necessary for the performance of Europol's tasks. Processing of information obtained from a comparison with Eurodac data is subject to the authorisation of the Member State owning the data.

Screening Regulation
According to the newly adopted Screening Regulation 2024/1356, third-country nationals who: are apprehended in connection with unauthorised border crossing, who are disembarked after search and rescue (SAR) or apply for asylum at border crossing points, as well as irregular migrants who had crossed borders in an unauthorised manner and are found in Member States' territory, will be subject to identification and security checks, in order to establish or verify their identity and check whether the person might pose a threat to internal security. Those persons' biometric data will be registered in Eurodac. Identity checks will be run against the Common Identity Repository (CIR), which includes identification data of persons registered in the EES, VIS, ETIAS, Eurodac and ECRIS-TCN, and the Schengen Information System (SIS). Verifications for security purposes will be carried out against the VIS, the EES, ETIAS, including the ETIAS watchlist referred to in Regulation (EU) 2018/1240, SIS, ECRIS-TCN as regards persons convicted in relation to terrorist offences and other forms of serious criminal offences, Europol data processed for the purpose of cross-checking as referred to in Regulation (EU) 2016/794, Interpol's Stolen and Lost Travel Documents (SLTD) and Interpol's Travel Documents Associated with Notices database (TDAWN). After the screening, the competent authorities should complete a form containing, inter alia, whether the consultation of the relevant databases resulted in a hit. This form, including the information on whether the database search resulted in a hit, is then transmitted to the authorities registering the

applications for international protection or to the authorities competent for return procedures, depending on which authorities the person is referred to.

5. ENTRY EXIT SYSTEM (EES)

Which authorities can consult the EES for law enforcement purposes?
National authorities which are designated by Member States pursuant to Article 29 of Regulation (EU) 2017/2226[34] are entitled to consult EES data for the prevention, detection and investigation of terrorist offences or other serious criminal offences. The conditions for access to EES data by designated authorities are specified in Article 32 of the Regulation.

Access is permitted if: it is necessary to prevent, detect and investigate terrorist offences or other serious criminal offences; it is necessary and proportionate in a specific case; and if there is evidence or reasonable grounds to believe that accessing EES data will contribute to these objectives. This is particularly relevant when there is a substantiated suspicion that the suspect, perpetrator, or victim falls under a category covered by Regulation (EU) 2017/2226.

Which data can be searched in the EES?
Consultation of the EES for the purpose of identification is limited to searching in the individual file with any of the following EES data: fingerprints of visa-exempt third-country nationals or holders of a Facilitated Transit Document. In order to launch this consultation of the EES, latent fingerprints may be used and may therefore be compared with the fingerprints stored in the EES as well as facial images.

Procedure to consult the EES for law enforcement purposes
Access to the EES as a tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence is allowed after a prior search has been conducted in national databases and, in the case of searches with fingerprints, a prior search has been launched in the automated fingerprint identification system of the other Member States under Decision 2008/615/JHA where comparisons of fingerprints are technically available, and either that search has been fully carried out, or that search has not been fully carried out within two days of it being launched. Exceptions to the general conditions are made in cases of urgency where there is a need to prevent an imminent danger to the life of a person.

Access to the EES by Europol
Europol must designate one of its operating units as the 'Europol-designated authority' and authorise it to request access to the EES through the Europol central access point. One of the conditions for Europol access is that the consultation is necessary to support and strengthen action by Member States in preventing, detecting and investigating terrorist offences or other serious criminal offence falling under Europol's mandate. Access to the EES as a tool for the purpose of identifying an unknown suspect, perpetrator or suspected victim is allowed where the person in question has not been identified after consulting, as a matter of priority, the databases that are technically and legally accessible to Europol.

[34] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).

6. EUROPEAN TRAVEL INFORMATION AND AUTHORISATION SYSTEM (ETIAS)

Which authorities can consult ETIAS for law enforcement purposes?
Member States' designated authorities and Europol may consult data stored in the ETIAS Central System for the purposes of the prevention, detection and investigation of terrorist offences or other serious criminal offences falling under their competence under the conditions established in Regulation (EU) 2018/1240[35].

Which data can be searched?
Consultation of the ETIAS Central System is possible with one or several of the following items of data recorded in the application file: surname (family name) and, if available, first name(s) (given names); other names (alias(es), artistic name(s), usual name(s)); number of the travel document; home address; email address; phone numbers; IP address. Consultation may be combined with the following data in the application file to narrow down the search: nationality or nationalities, sex, date of birth or age range.

Procedure to consult ETIAS for law enforcement purposes
An operating unit within the designated authorities that are authorised to request a consultation of data stored in the ETIAS Central System can submit a reasoned request for consultation of a specific set of data stored in the ETIAS Central System. Each Member State will designate a central access point which will have access to the ETIAS Central System. The central access point will verify that the conditions to request access to the ETIAS Central System are fulfilled. If the conditions for access are fulfilled, the central access point will process the request. The data stored in the ETIAS Central System accessed by the central access point will be transmitted to the operating unit that made the request in such a way that the security of the data is not compromised. In the urgency cases, where there is a need to prevent an imminent danger to the life of a person associated with a terrorist offence or other serious criminal offence, the central access point will process the request immediately and will only verify ex post whether all the conditions are fulfilled, including whether a case of urgency actually existed. The ex-post verification will take place without undue delay and in any event no later than seven working days after the processing of the request.

Access to ETIAS by Europol
Europol may ask to consult data stored in the ETIAS Central System and submit a reasoned electronic request to the ETIAS Central Unit to consult a specific set of data stored in the ETIAS Central System.

7. WHAT OTHER MEASURES AND TOOLS COULD BE USED TO ACCESS 'MIGRATION-RELATED' INFORMATION?

Directive 2023/977[36] on the exchange of information between the law enforcement authorities of Member States establishes rules for the exchange of information between law enforcement

[35] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).
[36] Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA (OJ L 134, 22.5.2023, p. 1).

authorities of the Member State for the purpose of preventing, detecting and investigating criminal offences. The Directive must be implemented by the Member States by 12 Decembre 2024.

As provided for in Directive 2023/977, the Single Point of Contact (SPOC) established in each Member State is the central entity responsible for coordinating and facilitating the exchange of information under the Directive. The SPOC is the single, main contact point for law enforcement authorities at national and international level and it operates 24/7.

All exchanges of information under the Directive are subject to the general principles, namely those of availability, equivalent access, confidentiality, data reliability and data ownership.

For highly sensitive investigations and terrorism cases, the Directive provides for exceptions in Article 7(4)(b) allowing Member States to authorise their competent law enforcement authorities not to copy the SPOC into communications.