EUROPEAN
COMMISSION

Brussels, 16.4.2024
COM(2024) 173 final

ANNEX 2

ANNEX

to the

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions

State of Schengen Report 2024

ANNEX 2

Compendium of best practices identified in the framework of the Schengen evaluation and monitoring mechanism

The well-functioning of the Schengen area relies on Member States' effective and efficient application of the Schengen rules. The Schengen Evaluation and Monitoring Mechanism (SEMM) is a key safeguard to ensure the adequate implementation of the Schengen acquis, which allows not only for the timely detection of vulnerabilities, but also allows for the identification of best practices and innovative solutions put in place by Member States.

The compendium of best practices accompanying the 2024 State of Schengen Report marks its second edition since the new SEMM Regulation came into force. As a living document, it encompasses both the best practices identified in the previous iteration of the compendium, as well as new and innovative measures identified in the evaluations that took place in 2023.

The compendium of best practices brings together a wide range of best practices covering several aspects of the Schengen acquis, including national Schengen governance, management of the external borders, visa policy, returns, as well as measures within the Schengen area, such as internal borders and internal security. The aim is to provide insights into innovative strategies, tools, and measures that can support Member State authorities in the implementation of the Schengen acquis and to facilitate peer-to-peer knowledge sharing. Further exchange of knowledge and experience should be fostered within the relevant Council bodies to reinforce this collaborative effort. The compendium serves to complement existing best practices outlined in applicable Commission or Council Recommendations or handbooks with new insights.

This compendium is explanatory and has no legally binding status. It is intended as a valuable resource for policymakers, law enforcement officials, and other stakeholders involved in ensuring the smooth and efficient functioning of the Schengen area but also to support possible solutions for remedial actions addressing future recommendations proposed by evaluation teams. It is part of the annual report referred to in Article 25 of Council Regulation (EU) 2022/922.

NATIONAL SCHENGEN GOVERNANCE

1. National strategies

Implementation of European Integrated Border Management (EIBM)
Governance of national IBM - A centre bringing together seven authorities, including the police, the migration office and the customs administration is created at national level. Its main aim is to develop counter-strategies, provide early warnings and develop recommendations. It is a permanent structure, organised around the work of temporary units, and has a wide range of analytical products that serve both tactical decision-making at local level and strategic decision-making at ministerial level. Its analyses are distributed to all border police units through the police web platform. [*Germany, 2015*] - **The contingency plan includes detailed procedures for a variety of potential crisis scenarios, defines clear roles and responsibilities for all relevant national authorities (including police, customs, armed forces and immigration services), as well as local stakeholders (such as municipalities and non-governmental organisations). Such plans are further complemented with procedures for requesting and integrating European support. Several tests of the contingency planning framework were performed involving all national authorities with responsibilities in crises.** [*Finland, 2023*]
Quality control mechanism - The Ministry of the Interior has established a national evaluation mechanism for external borders, built on the European and national quality control mechanisms. It brings together the recommendations from the Schengen evaluation mechanism, Frontex vulnerability assessment and national evaluation visits. The latter includes an evaluation of the Schengen Information System/SIRENE and police cooperation issues. [*Austria, 2020*] - Border management at national and EU level should be systematically subject to the application of the European quality control mechanism covering the entire scope of the EIBM. The permanent national quality control mechanism includes a national evaluators' pool, which is trained in Frontex Schengen Evaluators' courses. [*Thematic Evaluation of national IBM strategies, 2020*]
Interagency cooperation
- Close and effective formalised inter-agency coordination and cooperation between the different national authorities at central, regional and local level are considered essential for the effective functioning of integrated border management systems. Border guard units are deployed in the territorial waters and on land of the third countries concerned, ensuring constant joint patrolling by sea and air on board vessels and airplanes of the Member State, supported by electronic means such as the integrated external surveillance system (SIVE). [*Thematic Evaluation of national IBM strategies, 2020*] - **The interagency sharing of intelligence information through the same platform, contributes to build a common structured picture that improves the quality of information sharing and supports the main stakeholders in the accomplishment of their institutional mission, avoiding the duplication of efforts.** [*Estonia, 2023*] - **Joint investigation cell established involving other national law enforcement authorities and five other EU members States affected by the migration flow, as well as Europol and Frontex. This allowed an effective and high-speed exchange of information, thus fast reaction, and effective**

measures to be taken to slow down the migration flow and carry out actions against the facilitators. Criminal intelligence and open-source information collection and concentration in this cell, cross checking of persons made the joint investigation cell an operational hub at the external border supporting the overall management of the phenomenon. [*Lithuania, 2023*]

2. National capabilities

Training
Cooperation with CEPOL - **Coordinated and active participation to European law enforcement training is an integral part of the inter-agency cooperation within the Police, Customs and Border Guard permanent governance structure. The training needs are regularly discussed not only by the Police University College, but also in constant cooperation with Border Guard´s and Custom´s training institutions. The participation in CEPOL courses is high and the access to the CEPOL e-learning platform LEED is granted to a wide number of law enforcement officers. CEPOL trainings are included in the national Police, Customs and Border Guard annual training plans and under the coordination of the Police University College, available CEPOL training seats are shared between the law enforcement authorities based on their needs and competencies. Moreover, the information concerning the possibilities of the CEPOL trainings are easily accessible at the police, Customs and Border Guard intranet.** [*Finland, 2023*]
Returns - An extensive training programme conducted by highly qualified trainers, along with an established framework for escorting, supported by a well-developed network of trainers, guarantees high standards of performing escorts in line with Frontex standards. The training consists of both theoretical and practical parts. The theoretical part focuses on return operations procedure, fundamental rights, - legal framework, communication and cultural awareness as well as medical aspects. During the practical part, officers get familiar with Intervention Techniques and Restraints Situation Training (First Contact, Briefing PIC, Boarding, Seating, Movement on Board, Unauthorised Movement, Catering, Lavatory Procedure and Handover). The practical exercises are done in an airplane mock-up, which makes it possible to train in realistic situations. [*Portugal, 2022*] - **Agreement with an airline company to use aircrafts and simulators in regular basis to train the pool of escorts on return operations, not only from an operational perspective, but also to simulate emergency situations that could take place during the return operations such as fires.** [*Finland, 2023*]
SIRENE Bureau - The national police service has strongly supported the development of well-designed e-learning modules that turned out to be particularly efficient in the pandemic context, to reach almost all end-users interested. Tools were also developed to monitor the progress of the training audience and refresher courses were introduced. This led to an average good knowledge among the end users of the Schengen Information System in terms of potentiality, functionalities and procedures to follow. [*Ireland, 2021*] - **The SIRENE Bureau of the National Bureau of Investigation has created a national online training course focusing on the new Schengen Information System Regulation. The course contains theoretical material and knowledge checks. The online training package is mandatory for Police**

officers, Border Guards and Customs officers and completion of the course is monitored and followed-up. [*Finland, 2023*]

- **Establishment of a state-of-the-art Training centre within the premises of the SIRENE Bureau, which provides a comprehensive practical training opportunities for all the end users of all national Law Enforcement Agencies. The educational activities include practical sessions in computer labs and the availability of e-learning platforms, including the Police intranet and CEPOL courses, related to SIS distance learning. The Police Academy regularly cooperates with the relevant departments in the Police, local Universities and NGOs to ensure that regular updates are included in the training programme, also in the field of international police cooperation and Schengen matters. A full set of Manuals containing with all relevant information on Schengen Information System, Automated Fingerprint Identification System and SIRENE matters for each competent national authorities and Police Services is available via e-libraries on the Police intranet.** [*Cyprus, 2023*]
- **The national IT system records information and documents about third-country nationals subject to return, thus giving a complete picture of their situation. The SIRENE Bureau is in charge of converting directly in the Migration authorities' systems the national alerts on return to alerts on refusal of entry and stay upon receiving R-A SIRENE forms from other Member States on national alerts. The same procedure can be performed by the border guards when the person, subject to a return alert is located at exit out of EU territory**. [*Estonia, 2023*]

Joint training with other Member States

- The Member State has embraced the concept of joint training with the police services of its neighbouring countries as a way to improve cooperation in the border areas. Joint trainings and other law enforcement agencies with foreign counterparts stem for instance from the work of the Bilateral Cooperation Committee. Joint trainings are also organised by the Police and Customs Cooperation Centre. [*Germany, 2020; Spain 2022*]

Data protection

- There is well developed data protection training for expatriate staff at Consular Posts and data protection training, which is organised in cooperation with the Ministry of Foreign Affairs' Data Protection Officer and the Data Protection Authority. [*Czech Republic, 2019*]
- Wide-ranging training concept of the National Schengen Information System controller and in particular, the provision of e-learning modules and the comprehensive training strategy for new staff members [*The Netherlands, 2021*]
- The data protection authority's (DPA) staff members working with issues related to Visa Information System (VIS) and Schengen Information System (SIS) receive appropriate training, which is customised for each person individually. [*The Netherlands, 2021*]
- **The comprehensive training on data protection requirements related to the Schengen Information System organised by the Data Protection Officer and provided for the National SIS and SIRENE Bureau staff members and end users, especially regarding awareness raising efforts.**[*Italy, 2021*].
- **The Ministry of Foreign Affairs training and awareness raising of staff on data protection requirements in relation to visa issuing procedure and to the Visa Information System, including the active involvement of the DPO Office, for end users, in particular for consular staff before posting to embassies/consulates.** [*Greece, 2021*]

Equipment
- The use of modern, tailor-made technical equipment like tablets, smartphones and other portable items, with dedicated software programmed to facilitate the work of the police in identifying third-country nationals, to swiftly verify whether the third-country nationals subject to police checks are entitled to stay in the Member State. [*Switzerland, 2018*]
Mobile devices
- The important roll-out of mobile devices has increased the overall number of searches and hits in SIS. [*Czechia, 2019*] - Use of a mobile device that checks the readable zone of the travel documents, shows and stores the data from documents, and searches national databases and the SIS. In case of a breakdown of the query systems, mobile devices with document readers can be used to check the SIS for passenger traffic control. [*Hungary, 2019*] - Mobile devices have been deployed to provide patrol officers with access to relevant databases via a mobile application. Both user-friendly and powerful, mobile devices can read vehicle licence plates as well as the Machine-Readable Zone (MRZ) of identity documents. They are also equipped with facial recognition capabilities (i.e. send photographs for facial recognition purposes to a central database). [*Hungary, 2019*] - The distribution of mobile devices equipped to query in the Schengen Information System ensures that all police officers can easily and swiftly query the system by themselves no matter where they are. [*Belgium, 2021*] - All police officers with the relevant profile have been equipped with smartphones with direct access to (inter)national databases and with a secure communication application. The national police forces use a mobile solution for working outside the office. Via mobile devices (tablets, smartphones and laptops), every operational police officer can query (inter)national databases (such as identity documents, license plates and biometrics). Objects, such as license plates, which are scanned with the smartphone, are immediately checked against the central database. [*The Netherlands, 2021*]

3. Large-scale IT systems

National applications
Alerts and queries
- If the SIRENE Bureau creates, updates or deletes an alert using the national application, the issuing/requesting authority is automatically notified using an automatic email notification. This simplifies the procedure, reduces the workload and improves the exchange of information between the different authorities involved. [*Hungary, 2019*] - The Member State receives passenger data from all flights coming from third countries, the Targeting Centre Borders compiles it and the data is processed automatically through the national Advance Passenger Information (API) System. The API System consists of national databases, 'watch lists', profiles based on risk analysis, the SIS and the Stolen and Lost Travel Documents (SLTD) database. In case of a match, the operators have access to several databases and use the national application to verify the match and get more information about the alert (photographs, fingerprints, more details about the 'action to be taken', etc.). The hit result displays identifiers, 'reason for request' and 'action to be taken'.

The suspect's data and flight details are sent to the relevant airport or seaport which is responsible for apprehending the suspect. [*The Netherlands, 2021*]

- All SIS query applications provide an easy possibility (a small red button right under the name of the end-user) to see the information on data quality warnings on SIS alerts created per office (by office code), which can be an easy way to rectify errors in the national SIS alerts. [*Italy, 2021*]
- **Besides the owners of firearms, all imported firearms also have to be registered by the importers and dealers in the police register with the same automated queries being made. Since August 2022, it has become mandatory to upload photos of the firearms indicating all available markings and serial numbers. This ensures that the photographs are available for attachment to alerts if a weapon is being entered in the Schengen Information System.** [*Lithuania, 2023*]
- **The centralised search application used for querying the Schengen Information System by police officers and other end users is very straightforward and user friendly, with a clearly visible display of the linked alerts. The application provides for seamless transition to the linked alert.** [*Finland, 2023*]

Hit reporting

- Several practices are in place to ensure the automatic notification of a hit to the SIRENE Bureau. In particular:
    - Displaying of information on second line officer's screens on a hit as soon as it is registered in the first line. The border guards in the SIRENE Bureau also receive information on hits via the border guard application. [*Poland, 2015*]
    - When the National Road Vehicle Agency achieves a hit, the SIRENE Bureau receives an automatic e-mail notification. This allows the SIRENE operator to verify the hit and contact the Agency in case the latter has not taken the initiative. [*Luxembourg, 2016*]
    - The border application has a direct 'chat' functionality with the case handler in the SIRENE Bureau, which allows immediate direct contact with the SIRENE Bureau if an internal hit reporting form is sent off. [*Croatia, 2018*]
    - The national application allows the end user to send instant messages (i.e. from first to second line) to provide further details about the hit. [*Finland, 2018*]
- A standardised hit reporting form is available to all end users. End users can access this form directly via the applications used to query SIS at the state level or by the file-handling system of the Federal Police. The hit form is interactive and can be easily completed using the values provided in the drop-down menu. It also identifies erroneous information entered in the free-text fields. [*Germany, 2020*]
- At the airport, border guards have set up an effective follow-up procedure for hits on discreet check alerts in cooperation with customs officers. When border guards notice that a passenger is subject to an SIS request for a discreet check, they will discreetly signal this to customs officers. [*France, 2021*]
- **The national application provides the Schengen Information System alerts hit reporting form for the end users, with a pre-filled template which retrieves from the alert all the available data. The end users fill out the hit relevant fields and send it directly to the SIRENE Bureau, a received email message includes HTML format, which can be directly converted into a SIRENE form. Inquiry check questions are prefilled in the hit-reporting form. This ensures a very good level of data quality and hit reporting in real time.** [*Lithuania, 2023*]

- **Effective procedure to report that a person who is subject to a return decision and return alert has left the Schengen area. In such cases, the border guard authority which had the hit records the departure directly into the application used by the Migration Service. The SIRENE Bureau deletes the return alert and introduces the refusal of entry alert outside office hours when the information of the departure is received from other Schengen Member State or the national Embassies or Consulates. In cases of forced return, the local police units which executed the forced return also record it directly in the system. Such procedure ensures an effective management of the return policy at national level and also ensures that the refusal of entry alert is introduced to the Schengen Information System without delay when the return decision is accompanied by an entry ban.** [*Finland, 2023*]

Alert creation

- In the SIRENE workflow, a warning message was created to remind the authorities of the necessity to insert biometrics if available when creating an alert in SIS. [*The Netherlands, 2021*]
- When creating SIS alerts via the national application, data from previous records are automatically added. Photographs are attached and identity details can be automatically inserted into the new alert. [*France,* 2021]
- **High level of data quality and automation in two processes in the Register of Wanted Persons. First, when an alert on a national is created, the register automatically checks whether there is a vehicle, or a firearm registered in the national databases to the name of the person and automatically offers to the end-user the possibility to include the object as an extension to the alert, which needs to be confirmed by the end-user. Second, when entering an alert on a resident, the register pre-fills and imports the alphanumeric data (including the ID document information) in the alert from the national registers (the photograph of the ID document is not uploaded automatically, but added manually, when available). In addition, when creating a return alert in the national application on a person whose personal information is in the national registers, the national application imports the alphanumeric and biometric data in the alert as well (including the copy of the ID document, when available).** [*Lithuania, 2023*]

National SIS, National VIS and IT systems

- An alert system is available to signal anomalies immediately. The monitoring tool sends emails to system administrators in the event of an anomaly. [*Italy, 2016*]
- The Security operation centre monitors the security at user's level of the entire police network, detecting anomalies that might indicate possible attacks. When the Security operation centre detects a suspicious use, the Operation centre has to intervene to verify the possible anomaly. The active monitoring of 'atypical behaviour' from the end users performing queries allows them to identify signs of improper use of the Schengen Information System and to prevent possible data security risks. [*The Netherlands, 2021*]
- In the national IT visa system, urgent applications (e.g. in a case when an applicant needs to travel very shortly following the submission of the application, such as hospitalisation of a close family member) are permanently flagged. Therefore, urgent applications are easy to identify and their examination can be easily prioritised. [*Malta, 2022*]

- **The monthly data quality reports produced by eu-LISA are received at the National Schengen Information System Office and are then, prefiltered to include only the alerts that the SIRENE Bureau needs to check and/or forward to the end users who have created the specific alert. The two-tier verification of possible errors ensures to a high degree the good quality of the data entered in the Schengen Information System by the authorities.** [*Lithuania, 2023*]
- **The National SIS application displays in a prominent manner "Immediate reporting" and "Misused identity", by placing the text at the top of the alert, highlighted in red letters. Such a display allows the end user to be instantly aware of the situation in terms of urgency, complexity and sensitivity of the alert.** [*Cyprus, 2023*]
- **The visa processing IT infrastructure significantly facilitates the submission and examination of visa applications in a secure manner, limiting the dependency on the external service provider concerning the management and control of the systems. First, an online visa application form available at the Foreign Ministry's website and used approximately in 80% of the visa applications, including a "Guide" with useful explanation in many languages regarding the data to be inserted into the different fields. At the end of the process it is possible to generate a checklist for the necessary supporting documents depending on the place of submission of the application and the purpose of the journey. Second, data entry system developed for the external service provider for registering applications and combining them with biometrics and scanned supporting document and fully managed by the national authorities. Finally, the "core" application processing system for the examination of applications and decision-making has an intuitive, user-friendly interface, allowing the decision-makers to easily contact the consulates, external service providers, border guards, and the police in relation to a particular application. The VIS Mail is integrated into the system in a user-friendly manner and the system has various analytical and statistical tools. The log management and control functionality of the system notifies the Ministry's support team of any unusual activities of users processing data.** [*Finland, 2023*]

Data Protection requirements in relation to the National Schengen Information System (N.SIS)
- Replies to data subjects from the authority managing the N.SIS are available in different languages. [*Denmark, 2017*] - The authorities managing the N.SIS accept data subject's rights requests made in languages other than the Member States' language. [*Lithuania, 2018*] - The Data Protection Officer of the N.SIS controller has established a comprehensive data breach notification policy, including procedures, tools and instructions to staff. [*Germany, 2020*] - Decentralised structure of personal data protection monitoring where contact persons for the issues regarding personal data protection are available in every unit of the police whilst two data protection officers (DPOs) are in charge of general supervision. [*The Netherlands, 2021*] - The Data Protection Office of the Central Directorate of the Criminal Police made extensive efforts to enhance data protection and data security, as well asfor the N.SIS, including by the design of policies on data protection and information/cyber security issues, the definition and the auditing of information security and data protection management system and the accountability on awareness and training on data protection. The Data Protection Officer is in charge of performing vulnerability management, coordinating the vulnerability assessment activity and performing risk assessment and auditing; he/she cooperates with the data controller in a proactive and collaborative manner, e.g. regarding the project

for the realisation of a Cyber Security Operation Centre that allows a prompt and effective incident management [*Italy, 2021*].

- The Police has established comprehensive information security and data breach notification policies, including procedures, tools, and instructions to staff, as well as business continuity documents. [*Norway, 2022*]
- **The user authorisation management of the National Police Board prevents unauthorised access to personal data. In addition to the situation where the post or tasks change, the superior of the user controls and assesses annually that the subordinates' user authorisations are appropriate and, if necessary, launches an internal procedure to update them. The responsible system coordinator must annually check that the user rights given to stakeholder groups and external persons are appropriate and updated.** [*Finland, 2023*]

Data Protection requirements in relation to the visa issuing procedure / Visa Information System

- The authorities managing the N.VIS accept requests made in languages other than the Member States' language. [*Lithuania, 2018*]
- The Ministry of European and International Affairs' multi-pronged (regular and comprehensive) approach to auditing the visa process in the framework of the Visa Information System. [*Austria, 2020*]
- Extensive activities of the N.VIS controller in relation to the supervision of the consulates and of the external service provider, including on data security and data protection issues. In particular, a series of self-audits were performed in the last years by the N.VIS controller. [*Spain, 2017; Italy, 2021*]
- **The Data Protection Officer of the Ministry of Foreign Affairs, European Union and Coperation is involved in the Ministry's inspections of the visa issuing procedure and is also in general strongly involved in many data protection aspects of the visa issuing procedure. [*Spain, 2022*]**
- Extensive log control carried out by an automated software tool to detect incidents in the log files. [*Denmark, 2022*]
- **The SIEM solution implemented in the IT system of the Ministry for Foreign Affairs is designed with numerous predefined rules triggering alarm and notifying by email the Ministry VISA support team in case of any unusual activity of users processing data in C-VIS. As the VISA system logs all processing of data in the VISA and C-VIS by all end-user authorities with access rights, the log control covers all those authorities, as well. The Ministry's Data Protection team has a well-established procedure for assessing data breaches and what additional steps need to be taken, including the timeframe for notifying the Data Protection Authority.** [*Finland, 2023*]

SIRENE Bureau

SIRENE procedures

- The Prosecutor's Office has a duty desk that is available 24/7 for referrals from the SIRENE Bureau. [*Denmark, 2017*]
- Involvement of SIRENE staff in on-spot activities during large-scale police operations. [*Switzerland, 2018*]

- A certificate is issued to the victims of misused identities in accordance with national procedures. [*Denmark, 2022*]
- There is a facility to submit fingerprints from the Schengen Information System to the national Automated Fingerprint Identification System through the SIRENE workflow system and get hit/no-hit responses automatically. This process is only initiated when a case file is created in the SIRENE workflow system. In accordance with the legislation, the process does not entail the storage of the SIS fingerprints in the national AFIS. [*Ireland, 2021*]
- **All relevant authorities related to the police internal secured network have their official dedicated mail accounts, used to exchange information. All police reports of incidents are visible to all offices with dedicated mail accounts, including the SIRENE officers who proactively search against the available databases, including the SIS, all EU and third-country nationals involved in the reported incidents. As a result of these queries, in case a positive match is produced, the SIRENE Bureau contacts immediately the Police station in charge of the case (that has reported the incident) and requests further action to be taken regarding the subject of the alert. The proactive approach developed by the SIRENE Bureau ensures that no hits are missed during the queries performed against the SIS.** [*Cyprus, 2023*]

SIRENE workflow system

- In the case-management applications, when there is a hit in an alert that contains aliases, misused identities and/or links, a window pops up highlighting the presence of this relevant information. This notification effectively addresses one of the most common problems among the query solutions in the different Member States: the difficulty of making this information visible to the end user. [*Hungary, 2019*]
- The SIRENE workflow system automatically checks all incoming messages from all international channels (including also SIRENE forms), against pre-defined keywords. Personal data included in the forms is automatically checked against the connected databases. Positive results from such screening are marked as 'hot hits' to indicate that those forms should be handled as a priority. Thanks to this solution, the SIRENE Bureau can effectively manage incoming requests without any backlog. [*Liechtenstein, 2021*]
- The workflow system contains many useful functionalities, including the possibility of direct messaging with the end users and vice-versa, shortcuts buttons for the most-used functions. [*Ireland, 2021*]
- Incoming A and M forms (used to exchange information on European arrest warrants and extradition requests, and on miscellaneous supplementary information when no procedure is laid down, respectively) on persons are processed automatically in the SIRENE case management system, which automatically transfers the incoming forms on alerts related to terrorism to the Danish Security and Intelligence Service. [*Denmark, 2022*]
- *The SIRENE* forms created by officers are pre-filled with alert data and have predefined texts available that can be added just with one click. The predefined texts are tailored for each form and type of alert. [*Slovakia, 2019*]
- **The SIRENE case management system is a single IT application that handles all messages in a highly automated way: incoming SIRENE forms are registered automatically to existing cases and assigned to the competent case officer; incoming A forms are processed automatically and checked against the national databases based on keywords. This process allows for all incoming A forms relate to these key words to be automatically sent once per day in a batch to the relevant**

departments and units. The A forms are assigned to an operator for manual handling only in case of a match. The dedicated national hit-forms are automatically sent from a preview window in the Schengen Information System alert by the end-users from the Police browser/registers and received in the ILO's incoming messages mailbox, and then converted into SIRENE hit-reporting forms. These processes significantly facilitate the performance of the tasks of the SIRENE Bureau and support the timely effectiveness of the exchange of supplementary information and forms. [*Lithuania, 2023*]

4. Fundamental Rights aspects

Forced-return monitoring
- Adequate monitoring is ensured by the full independence of the National Guarantor, the scope of its action, the trainings provided to the return escorts on fundamental rights (including on the rights of vulnerable groups of persons) and the principle of *non-refoulement*, as well as the regional network of trained forced return monitors operating on the whole territory. [*Italy, 2021*]
- The regular online publication of the forced-return monitoring reports by the Public Defender of Rights, including in English as part of the annual general report of the Ombudsman ensures an additional layer of scrutiny over the removal process, enhancing its transparency, and further supports the effectiveness of the forced-return monitoring mechanism. [*Czechia, 2019*]

5. Data protection supervision

- The Federal Data Protection Authority has developed tools for implementing regular supervision of the Federal Schengen Information System and Visa Information System authorities and carried out many supervisory activities, including yearly inspections at the Federal Schengen Information System end-user authorities. [*Germany, 2020*].
- **The Data State Inspectorate organises SIS and VIS supervision within the Business Process Model and Notation - a graphical representation for defining business processes in a business process model. Business Process Model and Notation allows employees to understand their responsibilities at each stage, as well as the entire process of supervision.** [*Latvia, 2023*]

EXTERNAL DIMENSION

Cooperation with third countries
Liaison officers - In the framework of their trilateral police agreement, the Member State has agreed to share all their Liaison Officers based in third countries and to target specific geographical target areas. [*Belgium, 2015*] - Under the Nordic police cooperation agreement national law enforcement authorities (Police, Customs and Border Guards) can use the entire network of Nordic Liaison Officers around the world. It is also possible for Member States to use Liaison Officers of other Member States. Furthermore, the cooperation between the Member State's police is enhanced by the deployment within the police department of one Member State. [*Finland, 2018*] - **There is a direct access from the International Liaison Office intranet to the Database of dactyloscopy data that allows the officers to query the national AFIS with a NIST file attached to an alert, allowing to retrieve any matches in a matter of minutes. When the automatic search results in a match, this match is also subject to a fingerprint expert verification. This functionality allows not only to query the national databases with alphanumeric parameters but also with biometrics, which increases the accuracy of the identification of the person**. [*Lithuania, 2023*]
International cooperation - The establishment of multilateral cooperation and bilateral agreements with several third countries allows data exchange in real time on maritime surveillance and in the border crossing points for the checks on ferries, and other border-related information. The authorities actively support the development of national capabilities for border control in third countries by donating assets. [*Italy, 2021*] - The national authorities manage the migration flows and tackle cross-border crime from outside the Schengen area through the implementation of a regional concept of border surveillance. It includes the deployment of liaison officers from third countries to the regional coordination centres of the Member State and vice versa, which aims to facilitate direct cooperation and exchange of information. Border guard units are deployed in the territorial waters and on land of the third countries, ensuring constant joint patrolling by sea and air. A search and rescue mechanism complements the regional border surveillance system with vessels coordinated by the national search and rescue agency. [*Spain, 2022*]

Visa Policy
External Service Provider - **Imposing financial sanctions on external service providers** in case of non-compliance with the contract, combined with reinforced monitoring of their work, is an effective way to bring the external service provider in conformity with the provisions of the contract and improve its performance. [*Austria, 2022*]

MANAGEMENT OF THE EXTERNAL BORDERS

National and European situational awareness and early warning system
Cooperation (situational awareness) - The gendarmerie of two neighbouring Member States developed very good bilateral cooperation under a memorandum of cooperation. Based on this memorandum it is possible to conduct joint patrols at sea and land and exchange operational staff, among others. The authorities of these Member States also agreed to integrate their maritime surveillance systems and to share information on the maritime situational picture. [*Portugal/Spain, 2017*] - The coordination between the National Coordination Centres of two neighbouring Member States allows for a common situational picture, efficient information exchange, improved situational awareness at the common borders and an increased response capacity, as the positioning of the assets is also shared between the two countries. [*Portugal/Spain, 2017*] - **The direct access to national databases (beyond those just used for border control) enables the National Coordination Centre to maintain a comprehensive national situational picture and ensure an enhanced situational awareness for its stakeholders at national and European level**. [*Finland, 2023*] - **The National Coordination Centre established a procedure for reviewing requests for activation of EUROSUR Fusion Services at the district and local levels. Such procedure verifies the legality and relevance of each request of EUROSUR Fusion Services, before they are submitted to Frontex, ensuring that only relevant and cost-effective requests for EUROSUR Fusion Services are sent to Frontex and then used in the operational activities**. [*Finland, 2023*]

Risk Analysis
Land borders - **The national risk analysis system of the border control institution is efficient and supported by functional inter-agency cooperation. Twice per year, the border control institution issues common risk analysis products with the Customs and the National Police. The regular and systematic exchange of information between relevant national authorities involved in the implementation of the European Integrated Border Management resulting in joint risk analysis products ensures comprehensive national situational awareness and supports adequate reaction capabilities. In addition, common trainings, joint operations, and tailored actions are organised between the relevant authorities involved in border management.** [*Lithuania, 2023*]

Border checks
Land borders - The shift leader delivers operational briefings to the officers assigned to first-line border checks before they carry out border checks on an incoming passenger high-speed train from a non-Schengen country. These briefings count on the participation of the customs representatives to ensure coherent information sharing on updated risk profiles as well as other relevant operational data. One team member of the border guard patrol was specifically trained for intelligence management. Effective border checks are carried out based on a strategic distribution of staff and adequate use of languages reflecting the

composition of the passengers. Advanced Passenger Information is required for all trains and for passengers and crew members on these trains. Nominated border guards process advanced passenger information included in the passenger list, pre-checked against pre-selected registers, assessing the flagged risks. Travel documents are examined and verified visually and utilising appropriate technical devices. [*Finland, 2018*]

Air borders

- A dedicated unit of six border guards monitors private transport and recreational aviation, including light aircrafts and helicopters, as it has access to real-time route tracking and flight data from the military radar. The unit receives all the flight plans which are then analysed. When the airport of departure or arrival is not a border crossing point, an alert is given to a police unit to intervene. In case of unauthorised landings at aerodromes not dedicated to border crossings, the authorities impose fines. Risk assessment of deviating flight routes is carried out regularly. [*Belgium, 2020*]
- **The communication between the first and the second lines at border crossing points at the airport via the national application is very highly automated and user-friendly. In case of a hit, the first-line officer has the possibility to type in comments in a dedicated field and the hit information together with the comments message is sent through the national application from the first line to the second line. When it comes to the e-gates, in case of a hit on a discreet check alert, the e-gate operator can also add a comment to the hit which is then immediately forwarded to the second line which collects additional available information and sends the hit form to SIRENE. This allows the check to be completed without any contact with the subject of the alert, while collecting the information needed.** [*Lithuania, 2023*]
- **Passenger Information Unit responsible for the collection and processing of passengers' data on all flights currently operating in the country. Its role is to inform (24/7) competent law enforcement authorities of the need to further examine incoming and outgoing passengers, after the automated comparison of their data with relevant databases (such as SIS, I24/7), or against abstract profiles modelled in cooperation and/or upon request of such authorities. As they receive queries from all law enforcement agencies, the unit is in a unique position to notice overlapping investigations and objects of interests and to inform respective agencies. Well-developed case management system for handling communications with competent authorities and Passenger Information Units of other Member States, established following international best practices, is at the heart of successful fulfilment Unit´s tasks and information exchange. The operations take due account of data protection and procedural requirements established by the relevant EU and national law. The Unit proactively runs awareness raising campaigns on the capabilities it offers. It is equipped with high quality technical and human capabilities.** [*Latvia, 2023*]

Border surveillance

- The border guards are supported by an operational system that allows direct mobile consultation of the relevant databases and operational coordination in border surveillance. The system is also used for the coordination of patrols, situational awareness, positioning of patrols and efficient reaction capability. It further allows the Regional Coordination Centre to have a general operational picture, offering the possibility to select the proper means of intervention and the channel of communication in due time. The interactive interface allows the border guard and police patrols, the shift leaders and the Regional Coordination Centre to select and send the geo-location of a place of interest directly to the monitors installed in each patrol car and vessel. It provides a constant and comprehensive situational awareness

to the border guards responsible for border surveillance, facilitates communication and improves the reaction capabilities. [*Estonia, 2018*]

- The border guard uses Unmanned Aerial Vehicles (UAV) for surveillance and intervention tasks. Each of the regional units responsible for the external land borders is connected to the system. It consists of three platforms (unmanned mini motor gliders), a ground station (with remote control, screens and antenna) and other supporting equipment. The platforms are equipped with daylight and night-vision cameras, and one platform can be used at any given time. High-quality images from the cameras are delivered in real-time either to the ground station or other connected recipients. This UAV system can enhance the border surveillance capacity, improve situational awareness and facilitate reaction capacities. Once a flying object is detected, the Regional Coordination Centre is swiftly informed for specific intervention measures to be conducted. [*Poland, 2019*]

National database for border surveillance:

- **The national border surveillance concept is based on a comprehensive and efficient national database, combining all the relevant functionalities to support operational and tactical tasks. This system follows all elements of the operational cycle of border surveillance: providing support for information collection, reporting on the tactical and operational outcome of activities, planning of shifts, management and coordination of patrols and designing efficient reaction response in the field and providing coherent situational awareness. The software provides for a single service platform for all law enforcement thus ensures effective utilisation of resources in case of emergency and benefits of compilation of the situational picture in designated areas of responsibility. The software is linked with functions of the mobile IT environment of the patrol deployed at the field. Based on its comprehensive and coherent design, the system can be operated on local, regional and national level.** [*Estonia, 2023*]

RETURN

Effectiveness of the national return system
Return procedures

- The practice of taking return, removal and entry ban decisions in one step reduces the administrative burden while the procedural rights of the returnees are fully respected. [*Austria, 2015*]
- The procedure of notifying the 'intention of issuing an entry ban' when an irregular stay is detected during exit checks, giving the third-country national the opportunity to raise objections, allows the authorities to issue an entry ban without interrupting the departure of the third-country national while respecting the third-country national's rights. [*The Netherlands, 2021*]
- The procedure established for systematically controlling the compliance of a third-country national with the obligation to return within the period for voluntary departure includes:
    - If the above checks do not yield results, the State Border Guard Service visits the last known address of the third country national in the Member State;
    - The Migration Department is informed of the results and takes appropriate measures. [*Lithuania, 2018*]

Forced-return procedure

- Procedures are in place enabling authorities to take a fast decision on a subsequent asylum application lodged during the removal process to avoid postponing or delaying the removal of a third-country national while ensuring effective implementation of the principle of *non-refoulement*. [*The Netherlands, 2015*]

Voluntary return

- The promotion of assisted voluntary return programmes at every stage of the asylum and return procedures ensures that third-country nationals are fully informed about the possibility to return voluntarily from the earliest contact with national authorities. This practice contributes to the high rate of voluntary return, which promotes a more dignified, safer and cost-effective manner to return irregularly staying third-country nationals. [*Luxembourg, 2016*]
- Throughout the entire return process, voluntary return is a priority for the national authorities. There is a proactive approach to motivate third-country nationals for voluntary departure during all stages of the procedure, particularly at detention centres. The detention centres are considered conducive to promote voluntary return, with case managers and authorities actively motivating third-country nationals to leave the country voluntarily, while providing adequate accommodation and support. [*The Netherlands, 2021*]
- The early engagement with returnees when promoting voluntary return/departure and the possibility for a returnee to participate in a voluntary return scheme at any point of the return process, promotes and increases the use of voluntary return and reintegration as an integral part of a common EU system for return in line with the EU strategy on voluntary return and reintegration. [*Denmark, 2022*]

IT system

- The use of high-end technology, mobile devices and comprehensive databases for easy access and exchange of information favours the effective return of third-country nationals with no right to stay. [*The Netherlands, 2021*]
- The national IT return case management system, which was developed in line with the Frontex model (RECAMAS), provides return-related authorities with an efficient and integrated tool, favouring the effective management of return cases. [*Italy, 2021;* ***Estonia 2023***]
- The connection of the national migration case management system to the Frontex Application for Return (FAR) charter flights module allows national authorities to reach directly all charter operations organised with the support of Frontex, and help them to organise and participate in return operations more efficiently. [*Austria, 2020*]

Detention for the purpose of removal

Detention centres

- A children's room in registration facilities for foreigners provides appropriate and stimulating surroundings for children. The long opening hours and accessibility without restrictions, the presence of a social worker and the large amount of games and activities available make it attractive for children to use. [*Lithuania, 2018*]
- Family centres and targeted psychiatric facilities can cater to the particular needs of vulnerable persons in detention. The family centre's layout, activities and staff commitment allow for family life as close as possible to normal and provide appropriate and stimulating surroundings for families and

unaccompanied minors. The psychiatric facility provides for close cooperation between the relevant partners to address the needs of vulnerable persons with psychological problems in the return process while increasing the efficiency of return procedures. [*The Netherlands, 2021*]

- The developed protocols and training of the personnel, combined with the design and the regime contribute to mitigating the stress and trauma for minors in the return process and are in line with the best interests of the child principle. [*Norway, 2022*]
- **The facilities for foreigners have mental healthcare offices, offering third-country nationals assistance with mental health issues such as post-traumatic stress disorder and prevention of suicide as well as supporting their adaptation. The psychologists carry out an initial appraisal with all new arrivals and inform them about the possibilities of seeking psychological support within the facility. This allows for the early identification of psychological issues, which can guarantee an effective approach and handling of such cases. The mental healthcare offices can be accessed during office hours from Monday to Friday after an appointment by phone or with an application form. This helps create an open and safe environment, especially when dealing with victims of trafficking and other vulnerable persons.** [*Lithuania, 2023*]

INTERNAL BORDERS

Cross-border cooperation in internal border areas
Operational cooperation with neighbouring Member States

- Joint trilateral patrols on trains with its neighbours. [*Austria, 2015*]
- A bi-annual joint crime analysis report and an operational crime analysis report are prepared between Member States on a fortnightly basis. Further, a daily briefing with information on crimes committed in one Member State is prepared and shared with the partner Member States. [*Liechtenstein, 2015*]
- Within a border region police district, there is a joint analysis team. This consists of several agencies comprising police, customs, and border and criminal offices. The analyses are used to inform decisions regarding border controls, policing and customs matters. It was noted that analysis reports were used to brief officers in advance of joint patrols, including the determination of the days, times and locations where such patrols would take place. For the ports authorised for non-Schengen arrivals, monthly risk analysis reports are compiled. These are used to inform the operational as well as the administrative aspects of the border controls. [*Denmark, 2017*]
- To ensure effective cross-border cooperation and mutualisation of resources, neighbouring Member States signed an agreement on the Common use of Covert Human Intelligence Sources to carry out undercover intelligence operations through a common pool of police officers. [*Lithuania, 2018*]
- The bilateral agreements on police cooperation concluded with two neighbouring Member States enable the exchange of information on administrative offences, provide for the transfer and transit of persons through the territory of the other state by officers of the other contracting party, contain provisions extending the traditional scope for cross-border hot pursuit and surveillance and grant the same police powers as a national police officer when the other Member State police officers carry out their activities on their respective territory. These agreements also organise a wealth of cross-border joint police cooperation initiatives. [*Czechia, 2019*]
- The national data system delivers screen flashes when an operation starts thus immediately alerting operators for necessary follow-up. It also provides live feed. The geolocation of the patrolling cars is

also visible in the system. Both the Police Cooperation and Customs Centres and the SPOC have direct access to it. [*Czechia, 2019*]

- Bilateral agreements in force with neighbouring Schengen countries allow cross-border hot pursuits in the respective territories without any time and territorial restrictions, as well as give permission for hot pursuit beyond offences mentioned in Article 2 of Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, for example, if someone avoids police or border checks. The bilateral agreements go also beyond the Schengen Convention provisions by allowing hot pursuit on water as well by allowing the apprehension of the pursued person by the foreign police officer carrying out the hot pursuit. According to the agreement, hot pursuits can be carried out through more than one Schengen internal border. [*Slovakia, 2019; Hungary, 2019*]
- The Member States cooperate successfully in cross-border surveillance with the neighbouring countries in cases of tracking GPS devices upon international requests. All neighbouring countries have technically compatible devices, which ensure the successful tracking of vehicles without physical surveillance. The central office coordinates the execution of such cases and keeps comprehensive statistics. [*Hungary, 2019*]
- Joint bi-national brigades to combat illegal immigration and smugglers are integrated and permanent international cooperation mechanisms enabling two neighbouring countries to organise controls based on shared analysis of migration risks. Composed of an equal number of officers from both countries selected for their technical and linguistic skills, these "brigades" (or "joint units") set up at the Franco-German and Franco-Italian borders are either governed by the Prüm agreements or by a bilateral agreement. In addition to the organisation of joint patrols, the joint brigades (or joint units) provide joint training. This joint brigade system facilitates the exchange of information between two neighbouring countries and the coordination of control operations and should therefore be encouraged and extended to other borders in particular the French-Spanish border. [*France, 2021*]
- **At the regional level, cross border cooperation is based on administrative protocols with competent authorities of the neighbouring Member States, which are further implemented through annual action plans. This practical cooperation covers joint risk analysis, joint operations and patrols, managing of specific events and joint trainings. Joint patrols are planned on a regular basis. This cooperation concept creates good basis for a joint operational response at the regional level, common use of limited resources and more comprehensive crime situational picture.** [*Estonia, 2023; Latvia, 2023*]

INTERNAL SECURITY

National Strategies on Law Enforcement
- Every four years, the Minister of Justice and Security sets the National Security Agenda with national policy objectives for police duties. On a regional level, the local government translates the national priorities into regional policy objectives for the police in the Regional Security Agenda. Law enforcement agencies exchange intelligence and information to gather appropriate information and intelligence to contribute to the National Security Agenda, the Regional Security Agendas and Europol's Serious and Organised Crime Threat Assessment (SOCTA). Steering Committees from the Research Department are tasked with the coordination and monitoring of the whole procedure. A daily operational briefing allows the different police teams to be informed about the specific points of attention in their working field. The briefing is based on a national model and provides all relevant information and intelligence available on local, regional, national and international level. Various threat assessments are

also elaborated. They are used for instance as a starting point for policymaking in the fight against organised crime and estimating threat levels that indicate the likelihood of a terrorist attack. Additionally, the Research and Analysis desks of all Regional Intelligence Services make their own threat and security assessments. [*The Netherlands, 2021*]

- **The Office of the Prosecutor General appointed a liaison prosecutor to the SPOC who is frequently consulted on flagging of alerts and international arrest warrants, complexed international criminal investigations and any other cases, where the prosecutorial input is needed.** [*Portugal, 2022*]
- **Very close cooperation between the Foreign Liaison officers and the central authority for international judicial cooperation who can advise and assist in writing European Investigation orders or Mutual legal assistance requests addressed to the Member State.** [*Portugal, 2022*]
- **Use of an analysis tool by the Police in its criminal analysis units, allowing for the establishment of 'profiles' of crime phenomena, based on operational data, which show the user an interactive visualization of said phenomenon, its trends, modi operandi and evolutions. Since starting the roll out of this application in 2019, the Police has significantly extended the number of analysed crime phenomena and of users.** [*Lithuania, 2023*]

Organisation of the Single Point of Contact (SPOC) for international law enforcement information exchange

Organisation, information exchange

- For better coordination of international police cooperation, the Police created a network of contact officers for international police cooperation. They are located in all Regional Police headquarters and the capital's Metropolitan Police headquarter. The contact officers function as a link between local police officers and the SPOC in National Police headquater when performing the following tasks: advising on the choice of channel for police cooperation, assisting in drafting the information exchange requests, translating, and transferring the replies to the local police, raising the awareness of local police officers of different international information exchange possibilities. The contact officers help to improve the quality and facilitate the coordination of information exchange requests. [*Poland, 2019*]
- There is a well-established daily flow of criminal incidents reporting from the local to the regional and state levels. In practice, an e-report on the events of the last 24 hours is regularly available to the local station management team, the regional level and the State Central Criminal Police Office. It allows all levels to take informed decisions. [*Germany, 2020*]
- The system for the coordination of counter-terrorist operations gathers all the intelligence from the different police organisations and institutions responsible for preventing and countering terrorism, violent radicalism, organised and serious crime. The system presents an adequate alternative, combining information management with operational coordination in a situation where the relevant national authorities do not have access to each other's databases. [*Spain, 2022*]
- **Deployment of international case officers at regional level in different Police Departments. These officers are part of the Single Point of Contact and have four weeks training on large-scale IT systems, exchange of supplementary information through the SIRENE channel, management of biometrics and field visits to Europol and Eurojust. They have full access to the case management systems of the Single Point of Contact, Interpol's I-24/7 secure global police communications system and have rights to introduce Schengen Information System alerts and Interpol notices.**

They also have access to the relevant systems and permissions equivalent to a case officer attached to the national SIRENE Bureau and the International Communications Centre. This has resulted in having expertise on the Schengen Information System available in each local division. Furthermore, the international case officers verify both quality and legal relevance of the requested information, draft SIENA messages to be sent to Liaison Officers at Europol and provide training, on international police cooperation within the local Police Department. [*Finland 2023*]

Organisation

- The permanent Police, Customs and Border Guard Crime Intelligence and Analysis Centre is a form of effective cooperation and coordination between the law enforcement authorities producing, among others, common analytical and threat assessment products. As such the PCB can be seen as a linchpin supporting both the policy level in taking evidence-based decisions based on a common situation picture as well as the regional and local services in their investigation and intelligence efforts. [*Finland, 2018*]
- Comprehensive and intensive cooperation between law enforcement agencies and the National Tax and Customs Administration both at national and regional levels. Joint investigations and operations as well as exchanges of information and data are common practices. [*Hungary, 2019*]
- Police Cooperation Centres have their own new state-of-the-art Case Management System module, which is integrated into the national CMS police system and has built-in functionality for generating comprehensive automated statistics on cross-border activities. [*Hungary, 2019*]
- The creation of Central Offices, pooling resources from different administrations and focusing on one type of crime, leads to very effective operational results. [*France, 2021*]
- Effective structure to produce not only the national threat assessment but also dedicated threat and risk assessments. It combines centrally organised quality control with requirement analysis at regional level. The multi-disciplinary strategic analysis unit is responsible for strategic crime analysis. The unit consists of a team working at the national level and field teams in several regions. Quality control is maintained at the central level which also ensures coherence between the different analytical products. The unit produces the annual national threat assessment which focuses on organised crime groups. [*France, 2021*]
- **Memorandum of understanding between the police and customs enables extensive cooperation between both administrations, which foresees for the exchange and sharing of relevant information and strategic, tactical and operational intelligence, in particular by facilitating mutual access to databases, with due regard for individual rights and data protection rules, development and promotion of best practices, procedures for operational matters with respect to joint actions, joint mobile patrol squads, joint investigation teams, joint intelligence teams, sharing of equipment between services and cooperation on the development, purchasing, deployment and use of technology**. [*Cyprus, 2021*]
- **The SPOC has a risk analysis group responsible for deeper analysis of national and international requests, received in SPOC, gathering additional information in available databases, and providing analysis reports on discovered crime trends, modus operandi. The reports are then forwarded to prosecutors and/or respective police agencies for supporting relevant investigations**. [*Portugal, 2022*]
- The International Cooperation Division combines operational information exchange with strategic decision-making at international level. This Division hosts the national Single Point of Contact for law enforcement international information exchanges. It benefits from representation from both national

police forces, regional police forces as well as customs. Both relevant authorities have a network of experts on international police cooperation, which assist and advise the criminal intelligence units at regional level on the use of the instruments of international police cooperation. The main law enforcement authorities train experts on international police cooperation regularly. These experts form part of their unit at regional level and perform this function in addition to their daily work. Knowledge is transmitted to the network at an annual meeting, where for example national Liaison Officers at Europol are invited as speakers. In between these meetings, knowledge about new procedures is transmitted to the network either via newsletters or *ad hoc* meetings. In addition, the experts of the authority's network receive a one week capability training before joining the network. These expert networks are a low-threshold way for the dissemination of knowledge on international police cooperation at the regional level. [*Spain, 2022*]

Use of Europol tools for cross-border cooperation and information exchange
- Data from the national system for police investigations is automatically uploaded into Europol's Information System. The database of ongoing investigations is connected to an automated data loader in Europol's Information System. New information is inserted, existing information is enhanced and old information is removed daily. This process is completely automated. The Europol National Unit handles hits occurring between national investigations and foreign investigations, already available within Europol's Information System. [*The Netherlands, 2021*]