



Council of the  
European Union

Brussels, 16 May 2023  
(OR. en)

9504/23  
ADD 2

JAI 635  
SCHENGEN 22  
SCH-EVAL 108  
FRONT 174  
IXIM 128  
MIGR 171  
ASILE 58  
ENFOPOL 248  
COMIX 242  
CORDROGUE 51

#### COVER NOTE

---

From: Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director

date of receipt: 16 May 2023

To: General Secretariat of the Council

---

No. Cion doc.: COM(2023) 274 final

---

Subject: 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 - **Annex 2 - State of Schengen Report 2023**

---

Delegations will find attached document COM(2023) 274 final Annex 2.

---

Encl.: COM(2023) 274 final Annex 2



Brussels, 16.5.2023  
COM(2023) 274 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 2023**

**EN**

**EN**

## ANNEX 2

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

*As the Schengen area without controls at internal borders (the “Schengen area”) continues to be a cornerstone of European integration, effective implementation of the Schengen rules is crucial for ensuring the smooth movement of people across borders, enhancing security while respecting fundamental rights, and fostering cooperation among Member States. The identification of the best practices and innovative solutions by Member States that could be applied by others is at the heart of the new Schengen evaluation and monitoring mechanism. Its objective is to improve the implementation of the Schengen acquis.*

*This compendium brings together a wide range of best practices and innovative solutions covering various aspects of the Schengen acquis, including border management, return, visa policy, law enforcement, data protection and the use of IT systems, which were identified during Schengen evaluations that took place during the implementation of the first (2015-2019) and second (2020-2022) multiannual evaluation programmes.*

*The compendium of best practices is intended to give insights into innovative strategies, tools, and measures that can support Member State authorities when implementing the Schengen acquis and to help them build further on proven approaches and techniques when putting forward new proposals and initiatives. It also aims to strengthen the framework, created in the relevant Council Working Party, to further facilitate and encourage Member States to share their experiences, exchange knowledge, and learn from each other. This would facilitate, in particular, peer learning and foster cooperation among Member States, leading to improved implementation of the Schengen architecture. The compendium does not intend to replace or repeat existing best practices included in the different applicable Commission or Council Recommendations or handbook but comes to supplement them with new items.*

*The Commission intends to update the compendium annually to harvest new and innovative measures identified by the evaluation teams during Schengen evaluation activities from the preceding year.*

*These best practices should also support the effective implementation of the multiannual strategic policy for European integrated border management (EIBM). Therefore, the Member States are invited to reflect the relevant best practices in their national strategies on integrated border management for EIBM.*

*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.*

## 1. Management of the external borders

### 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 creation of a well-functioning and permanent governance system for EIBM coordinated by a specific governing structure and comprising all national authorities involved is essential for the efficient establishment, monitoring and implementation of EIBM in the Member States. The involvement of the Frontex Liaison Officer (as an observer) in the national governance body for EIBM is considered beneficial for information sharing and effective cooperation, and to guarantee a connection between the national and the European level. [*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*]

#### Search and rescue

- The national strategy should address objectives to integrate the search and rescue (SAR) function in the national sea border surveillance concept and to make the link with the EU support in this area provided by the maritime joint operations coordinated by Frontex. The SAR function should be included as an integral part of the national sea border surveillance system in terms of planning and development of surveillance capabilities. The National Centre of SAR could share the information collected by the SAR World System to improve planning the surveillance. [*Thematic Evaluation of national IBM strategies, 2020*]

#### 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*]

### **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*]

### **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*]

### 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*]

### 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*]

## 2. 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*]

### National IT system

- 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*]

### 3. Return

#### Effectiveness of the 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. [*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:
  - Verification of the departure of the third-country national via border crossing points in the State Border Guard Service information system,
  - Consultation with neighbouring Member States’ competent authorities on whether the third-country national departed via their section of the external border;
  - 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*]

##### 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. [*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 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*]
- 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. [*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*]
- 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*]

## Safeguards

### 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 respecting the principle of *non-refoulement*. [*Netherlands, 2015*]

### 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 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*]

### Training

- 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*]



## **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. [*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*]

#### **4. Police Cooperation**

### **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. [*Netherlands, 2021*]

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

### Organisation, information exchange

- National systems are available across all law enforcement agencies, allowing to search each other's information, which reduces delays and increases efficiency. Furthermore, because all law enforcement agencies use the same national system to register cases, it prevents different law enforcement agencies from working on the same cases or missing opportunities for more cohesive working. [*Finland, 2018*]
- 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 headquarter 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*]

### Organisation

- The permanent Police, Customs and Border Guard Crime Intelligence and Analysis Centre (PCB) 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 (PCC) have their own new state-of-the-art Case Management System (CMS) 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]

- 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]

#### **Information Management – mobile applications**

- 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]
- 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. [Netherlands, 2021]

#### **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. [Netherlands, 2021]

## 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*]
- The Administrative Agreement on Cooperation between Police Authorities in the Nordic Countries provides for increasing operational police cooperation between the Nordic police authorities. The Agreement sets out guidelines for the exchange of information (to prevent, detect or investigate a criminal offence), police interviews in the jurisdiction of one of the other parties, requests for transcripts of criminal records and serving of subpoenas, search for a person in another Nordic country, Joint Investigation Teams, lending of equipment and transit in connection with extradition of foreign citizens. National police officers are well aware of the provisions that this agreement enabled them to utilise. [*Denmark, 2017; Finland, 2018*]
- 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]*

## Human resources

### Liaison officers (LO)

- 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]*

### Training

- 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]*

### Support of foreign police officers during events

- In case of special events (e.g. music festivals, Christmas markets, sports events and football matches), the police authorities based on Council Decision 2008/615/JHA use the support of foreign police officers. During a large festival the state police benefits from the support of uniformed police officers from other EU Member States, and special pickpocket investigators from other EU Member States. [*Germany, 2020]*

## 5. Large-scale information systems

### Schengen Information System (SIS)

#### 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]
- Extensive roll-out of the functionality that provides for searches based on fingerprints in national and SIS Automated Fingerprint Identification System (AFIS). This functionality and the fingerprint readers are available in most police stations. [Germany, 2020]
- 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. [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]

##### 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]
  - End users can send a hit notification to SIRENE directly from the SIS alert review window (automatic email generation). [Lithuania, 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 structured reporting form is available to the first-line border control officers in the border control application; it is used for describing the circumstances surrounding the hit and sending this information to the second-line control. [Poland, 2019]



- 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*]

#### **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*]
- 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*]

#### **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. [*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*]

#### **National SIS 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. [*Netherlands, 2021*]

#### **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]

### **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]

## Training

- 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]
- A comprehensive handbook covering internal procedures for handling SIS alerts is available for SIRENE operators and most importantly can be accessed directly from the SIRENE case handling application. [Norway, 2017]

## 6. Data protection

- 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. [Netherlands, 2021]
- Wide-ranging training concept of the N.SIS controller and in particular, the provision of e-learning modules and the comprehensive training strategy for new staff members [Netherlands, 2021]
- 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. [Netherlands, 2021]
- 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]
- Replies to data subjects from the authority managing the N.SIS are available in different languages. [Denmark, 2017]
- The authorities managing the N.SIS and 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]
- 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]
- 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 several supervisory activities. [Germany 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]