Council of the European Union

Brussels, 26 November 2020
(OR. en)

13378/20
ADD 1

SCH-EVAL 188
DATAPROTECT 136
ENFOPOL 321
FRONT 332
MIGR 163
SIRIS 92
VISA 133
COMIX 549

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	25 November 2020
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2020) 327 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Accompanying the document Report from the Commission to the Council and the European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanism pursuant to Article 22 of Council Regulation (EU) No 1053/2013 First Multiannual Evaluation Programme (2015-2019)

Delegations will find attached document SWD(2020) 327 final.

Encl.: SWD(2020) 327 final

EUROPEAN
COMMISSION

Brussels, 25.11.2020
SWD(2020) 327 final

COMMISSION STAFF WORKING DOCUMENT

Accompanying the document

Report from the Commission to the Council and the European Parliament

on the Functioning of the Schengen Evaluation and Monitoring Mechanism pursuant to Article 22 of Council Regulation (EU) No 1053/2013
First Multiannual Evaluation Programme (2015-2019)

{COM(2020) 779 final}

CONTENT

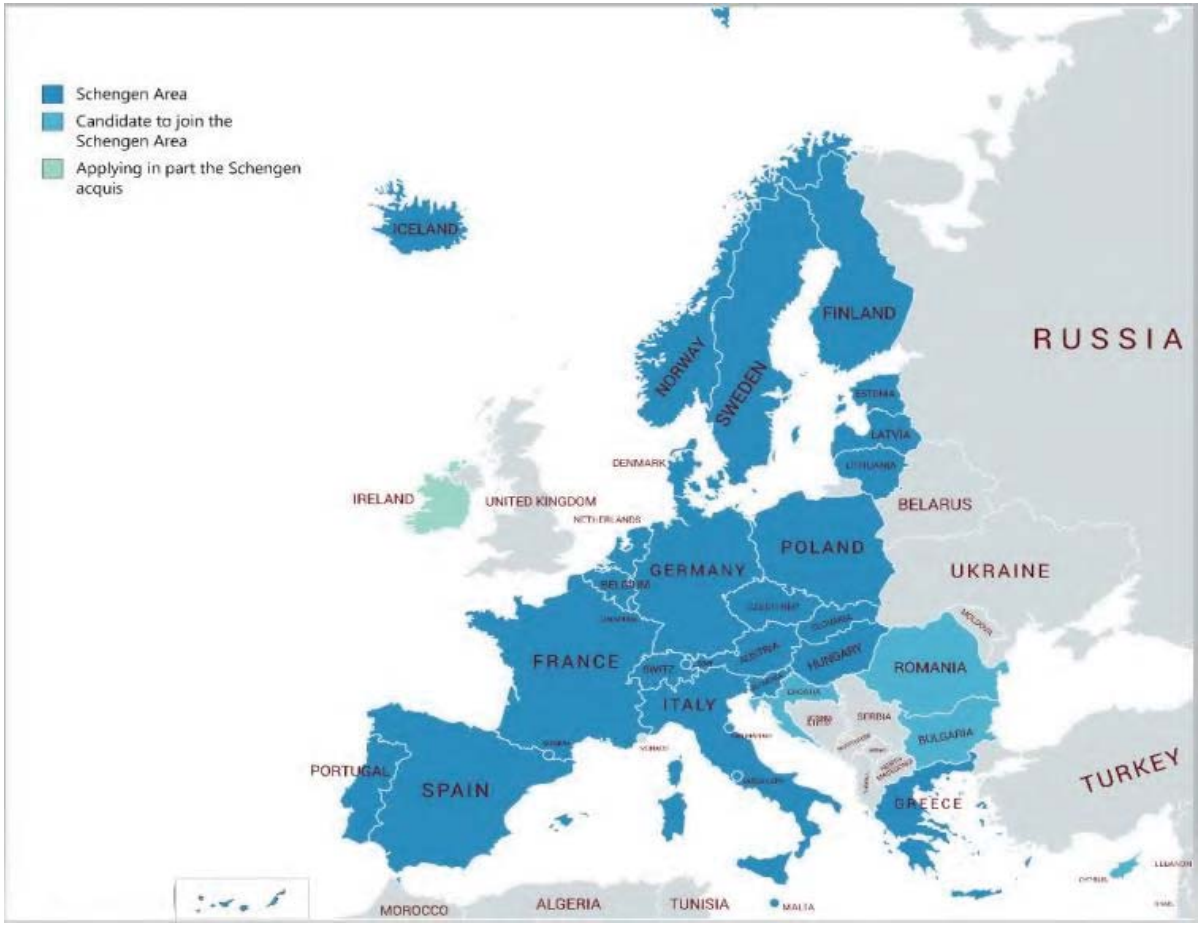
INTRODUCTION

This Commission Staff Working Document accompanies the Commission Report to the Council and the European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanism. The Report provides an overview of the mechanism and outlines the main recurrent findings in the different policy areas covered on a regular basis during the first Multiannual Evaluation Programme (External Border Management, Common Visa Policy, Return, Police Cooperation, Schengen Information System and Data Protection). It also discusses most recurrent procedural challenges encountered during these first Multiannual Evaluation Programme (2015-2019).

Part I of this document provides further details on the finding of the evaluations carried out while Part II reports statistics on the application of the main provisions of the SCH-EVAL Regulation[1] reflecting the situation on 5 November 2020.

[1] Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen, OJ L 295, 6.11.2013, p. 27 (SCH-EVAL Regulation).

Figure 1 – The Schengen Area[2]



[2] Beyond Member States, the Schengen area covers also Iceland, Norway, Switzerland and Liechtenstein (so-called 'Schengen Associated Countries'). Ireland is not part of the Schengen area but it will apply the Schengen *acquis* in part as of 1 January 2021. The United Kingdom was also not part of the Schengen area but applying in part the Schengen *acquis*. Bulgaria, Croatia, Cyprus and Romania are bound by the Schengen *acquis,* however, internal border controls have not yet been lifted in respect of these Member States. The report refers to all these countries as Member States.

PART I: SUMMARY OF THE FINDINGS OF THE SCHENGEN EVALUATIONS PER POLICY AREA

1. EXTERNAL BORDER MANAGEMENT

1.1. Introduction

A well-functioning area without internal border controls requires common, uniform and highly efficient external border management. Deficiencies in the external border management of one country can affect all Member States and subsequently put the functioning of the Schengen area at risk. Effective external border management therefore remains one of the main safeguards for an area without internal border controls and significantly contributes to guaranteeing the long-term security of the EU and its citizens. Common, uniform and highly efficient external border management is in the interest of all other Member States to facilitate smooth external border crossings of persons and goods, combat illegal immigration and other forms of cross-border crime such as trafficking in human beings, and prevent any threat to public policy, internal security, public health and international relations within the Schengen area. External border management evaluations are thus a key element of the Schengen Evaluation and Monitoring Mechanism.

The main legislative act governing this area is the Schengen Borders Code[3]. In the last five years, as a result of the new challenges faced by the EU, additional initiatives were introduced to reinforce this legislative framework, including systematic checks of EU citizens against relevant databases at external borders[4], the adoption of a new Frontex Regulation in 2016[5] and its subsequent review in 2019 with the inclusion of the EUROSUR Regulation[6], as well as the gradual development of an integrated system for managing the EU's external borders (the European integrated border management).

External border management evaluations cover the following main elements: external border checks at sea and airports and land border crossing points, external border surveillance, national strategies and concepts for European integrated border management, risk analysis, inter-agency and international cooperation, national quality control mechanism, external border management capacities (personnel and equipment) and infrastructure.

Between 2015 and 2019, evaluation visits were carried out in 25 countries of the Schengen area[7] as well as in Croatia and included also 12 unannounced visits and four revisits. In 2019, a thematic evaluation of Member States' national integrated border management strategies has started to assess the alignment of the strategies with the regulatory framework as provided by the Frontex Regulation.

---

3 Regulation (EU) 2016/399, OJ L 77, 23.3.2016, p. 1, as amended.

4 Regulation (EU) 2017/458, OJ L 74, 18.3.2017, p. 1, amending Regulation 2016/399 as regards the reinforcement of checks against relevant databases at external borders. The systematic checks of the travel documents of persons enjoying the right of free movement under EU law against relevant data bases was introduced.

5 Regulation (EU) 2016/1624, OJ L 251, 16.9.2016, p. 1. Repealed in 2019 by Regulation (EU) 2019/1896, OJ L 295, 14.11.2019, p. 1.

6 Regulation (EU) 1052/2013, OJ L 295, 6.11.2013, p. 11.

7 Liechtenstein was not evaluated in this area.

1.2. Recurrent deficiencies and areas for improvement

A core development in external border management during the first Multiannual Evaluation Programme was to prepare the implementation of the **European integrated border management concept**. To this end, specific focus was put on the evaluation of Member States' national policies at strategic level on integrated border management.

Almost all Member States have established a national integrated border management strategy and already implement in part or in full the European integrated border management concept. Yet the evaluations have shown that there is room for improvement in several Member States when it comes to coordination and cooperation in strategic planning and the strategic approach towards the capability development for external border management, including in human resources and training. Another aspect to be further strengthened by some Member States at national level is the referral mechanism at the external border for third country nationals seeking international protection to ensure the respect of the principle of *non-refoulement* and access to the asylum procedure.

A major aspect of European integrated border management is **interagency cooperation,** given the different actors involved in external border management in the Member States. The evaluations have shown that the overall interagency cooperation in the Member States works well, but in a few Member States, external border control authorities work independently, not sharing information, which prevents effective interagency cooperation at strategic level.

A unified approach to **risk analysis**, the main management tool for external border management, is guaranteed by implementing the Frontex Common Integrated Risk Analysis Model (CIRAM). This model ensures all Member States produce unified high-standard risk analysis products for external border management and return purposes. The evaluations have shown that not all Member States have fully implemented CIRAM. In some Member States sufficient institutional capacity to carry out risk analyses was not ensured as the number of specialised and trained staff performing this task was not sufficient. In a few cases, this negatively affected the quality of the risk analyses.

Deploying sufficient resources, including expert staff is essential to ensure an efficient, high and uniform level of external border controls. The evaluations found that most Member States face challenges related to resources, training and operational planning mainly at the local level (e.g. due to increased traffic flows at external border crossing points). However, only in few cases the shortages of trained staff negatively affected the overall **quality of external border control** at the national level. As for the training of border guards, the issues for improvement identified in several Member States relate to insufficient planning of trainings, in particular language training and implementation of continuous specialised training in core areas of external border control, particularly for detecting forged and falsified documents. In addition, Member States should ensure that temporarily deployed staff responsible for carrying out external border controls also receive the basic border guard training.

A number of recurrent deficiencies that could negatively affect the quality of external border controls and situational awareness relate **to border check procedures and the infrastructure** at external border crossing points. In some Member States pre-arrival information and results of risk analysis were not efficiently integrated in the external border control procedures. Other deficiencies include the limited checks on the purpose of stay and means of subsistence of third-country nationals and lack of information in all EU languages provided to a third country national subject to a thorough second line check as well as

insufficient infrastructure to ensure adequate profiling or to ensure the separation of the different traffic flows and to prevent individuals from circumventing external border checks.

External border surveillance, including situational awareness, is key to prevent unauthorised external border crossings and counter cross-border crime. Overall, the surveillance at the EU's external borders was considered satisfactory and in line with the legal requirements, but some areas for improvement were identified. In some Member States, the surveillance systems (e.g. radar stations and day/night cameras) did not cover all segments of the external border and an integrated and real-time situational picture at regional level was not always present and/or shared with the national level or other relevant external border control authorities. This could reduce the border guards' situational awareness and their ability to react, as well as the quality of the national situational picture.

With the establishment of a European Border Surveillance System (**EUROSUR**)[8] - an information exchange and cooperation framework between the Member States' Border and Coast Guards and Frontex – a European situational picture was created to improve situational awareness and to increase reaction capability at the EU's external borders. All Member States have established a National Coordination Centre (NCC) as provided by the EUROSUR Regulation and timely exchange of information via the system (e.g. national situational picture). Yet the National Coordination Centres do not always fulfil all their mandatory functions and the quality of the information provided was in some cases low, which prevents the EUROSUR Regulation from being implemented effectively and providing a comprehensive situational picture at the European level.

Allegations of fundamental rights violations at the external border in few Member State are a cause for concern and require close monitoring.

1.3. Points of particular interest

The evaluations identified many points of particular interest, in particular, the way technology is used to improve external border controls and increase situational awareness.

Some Member States' national border management information systems were considered to be very well-developed, supporting the border guards in their daily activities and having a positive effect on the quality of the checks that were being carried out. The increase in the use of state-of-the-art technologies for external border surveillance, such as drones and other equipment to identify unauthorised external border crossings, improves situational awareness and enables external border surveillance guards to better react to situations.

The efficient national quality control mechanisms (national Schengen evaluation and vulnerability assessment), covering all integrated border management elements and external border control authorities, contribute to identifying gaps and needs related to the efficient implementation of the Schengen *acquis*.

Specific external border check procedures have been established for vulnerable groups, in particular for (unaccompanied) minors, measures to counter trafficking in human beings, specific training methods for new border guards and the use of different bi- and multilateral international cooperation structures. These measures contribute to complying with fundamental rights and ensuring quality external border controls.

---

[8] Regulation (EU) No 1052/2013 (EUROSUR), OJ L 295, 6.11.2013, p. 11. This regulation has been repealed and its content has been integrated in Regulation (EU) No. 2019/1896 on the European Border and Coast Guard. Reference to the EUROSUR regulation should be understood as references to the European Border and Coast Guard Regulation.

1.4. Conclusion

Based on the 42 evaluations carried out in relation to external border management, it can be concluded that Member States are to a large extent adequately implementing the Schengen Borders Code and managing external borders in line with the *acquis*. While serious deficiencies were identified in four Member States[9], those Member States took swiftly the necessary measures to address the most important deficiencies. Today, no Member State has serious deficiencies in this area, but specific challenges remain in a few Member States that still need to be promptly addressed.

Decisive progress has been made during this first Multiannual Evaluation Programme to harmonise and align Member States' strategic approaches towards external border management by the gradual implementation of an integrated border management system.

Despite improvements made in the quality of border controls at the external border, Member States' external border management does not yet guarantee a uniform level of control at EU's external border given the diverging national practices and approaches to external border management. Some deficiencies need to be addressed and specific challenges remain in a few Member States that still need to be addressed.

The results of the evaluations have informed Frontex' vulnerability assessment and further developed the policy on European integrated border management as well as its implementation by the Frontex and Member States. Likewise, the evaluations' findings have been essential in amending the Schengen Borders Code to introduce the obligation of systematic checks (including against databases) and to strengthen Schengen standards.

2. COMMON VISA POLICY

2.1. Introduction

Inherently associated with external border management, the common visa policy has two main objectives. First, it enables Member States to conduct a thorough migratory and security assessment of third-country nationals who require a visa to travel to the Schengen area for short stays (up to 90 days in any 180-day period). Second, it also provides legal guarantees for applicants to ensure an efficient and fair visa procedure, with the aim of facilitating legitimate travel and people-to-people contact.

---

[9] The 2015 unannounced evaluation of **Greece** revealed serious deficiencies in particular due to the lack of appropriate identification and registration of irregular migrants on the islands, of sufficient staff, and of sufficient equipment for verifying identity documents. Under the current circumstances, situational awareness and reaction capability were not sufficient for efficient external border surveillance. The 2017 evaluation of **Iceland** revealed serious deficiencies in the carrying out of external border control by Iceland, in particular due to the lack of a strategic approach to external border management and an insufficient staffing and training level to cope with a sharp increase in the number of passengers and risks related to irregular migration. The evaluation of **Sweden** in 2017 revealed serious deficiencies, in relation to external border management in general (clear institutional set up, command and control functions, lack of national training system for border guards and lack of regular refresher training, risk analysis not in line with CIRAM 2.0). In the area of external border checks, the quality of the first line checks and the verification of the entry conditions of the third country nationals at most of the visited airports were not in line with the Schengen provisions while the number of staff at main airports was too low given the passenger flow. In 2017, the evaluation of **Spain** revealed serious deficiencies in relation to the capacity to perform external border checks in line with Articles 8 and 15 Schengen Borders Code at the external border crossing points of Ceuta and Melilla in light of the geographical location and migration pressure. Re-visits were carried out in Sweden and in Iceland in 2019.

The main legislative acts governing this policy field include the Visa Code[10] providing common and harmonised rules for visa processing, the Visa Regulation[11] listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement, and the Visa Information System (VIS) Regulation[12].

Between 2015 and 2019, evaluation visits – including also three unannounced visits – were carried out in 25 countries of the Schengen area[13] and Croatia. Evaluations on the implementation of the common visa policy take place mainly at the consulates in third countries. Some 55 consulates have been visited in 27 third countries as well as five central visa authorities in the territory of the Member States.

2.2. Recurrent deficiencies and areas for improvement

The **examination of visa applications** and assessment of applicants' migratory and security risk was found to be performed in a satisfactory manner. Overall, decisions on whether a visa should be issued or refused were well justified in most cases. In a few cases, standards of appreciation were applied too strictly or too leniently and recommendations were made to correct this.

Member States' **visa-issuing practices** still differ on whether single-entry visas or multiple-entry visas are issued, in particular for first-time travellers, and on the length of validity of the visas issued to regular travellers. This contributes to 'visa shopping'. It is still apparent that some consulates only consider applicants' visa or travel history in their country and do not take full account of visas issued by other Member States when assessing the application and deciding on whether the visa should be issued. Decision-making deadlines were mostly respected, but complying with the two-week deadline for obtaining appointments to lodge visa applications were not met by some consulates.

Visa officers' local knowledge combined with assistance from local staff speaking the local languages and regular participation in local Schengen cooperation meetings are essential for effectively processing applications. These conditions were not sufficiently met where decision-making has been centralised and takes place far away from where the visa applications were submitted. Decision-making by central authorities was considered to be non-compliant with the Visa Code. While the Visa Code has been amended in this regard and, as of February 2020, central authorities are also authorised to examine and decide on visa applications, the unintended consequences of centralised decision-making, in particular the loss of local knowledge and ability to closely follow developments and new trends in the applicants' country of origin, remain a concern for the Commission.

In the past years, several Member States have been put under pressure to make cost savings which resulted in **staff** shortages. The consequence is that in a number of cases, expatriate decision-makers had to process a high number of visa applications and some consulates are not able to meet the deadlines set out in the Visa Code, or that important tasks were transferred from deployed staff to locally hired staff. Although no specific risk was detected during the evaluations, such developments could affect the integrity of the visa procedure. In

---

10 Regulation (EC) No 810/2009, OJ L 243, 15.9.2009, p. 1, as amended.

11 Regulation (EU) No 2018/1806 OJ L 303, 28.11.2018, p. 39.

12 Regulation (EC) No 767/2008, OJ L 218, 13.8.2008, p. 60.

13 Liechtenstein was not evaluated in this policy area.

several cases, staff was also insufficiently trained, including on the use of IT systems and basic common visa policy documents.

The Visa Code allows Member States to outsource certain tasks related to the visa application procedure to **external service providers**, such as the collection of applications and biometric identifiers from applicants, and the return of travel documents. Recurrent deficiencies were found in relation to external service providers, for example, inadequate premises or security measures, long waiting times, insufficient staff training, excessively long retention of applicants' personal data or unsecured transfer of applicants' data from the external service providers to the consulate. In many cases, consulates did not sufficiently monitor external service providers. Unannounced spot checks and visits to visa application centres that are not located in the capital were rare. Member States only conducted a few monitoring activities jointly, despite visa application centres often serving several Member States. In a few instances, the evaluations revealed a worrying over-dependence on external service providers, with the latter controlling core elements of the visa procedure such as the underlying IT systems or the archive of applications.

The introduction of the **Visa Information System (VIS)** – a database supporting the exchange of data for short-stay visa applications — constitutes considerable progress for the visa procedure. The quality of the data in the Visa Information System, while generally satisfactory, could be improved. However, visa officers are still underusing the system. These factors lead to non-compliance with the Visa Code and the VIS Regulation on certain aspects, such as the delayed creation of application files in the Visa Information System, incomplete or incorrect data entered in the system, applications that are not grouped or linked, and generally a lack of awareness about the Visa Information System mail functions. Member States must take fingerprints from the same applicant only once every five years and must copy fingerprints from previous applications lodged in the previous 59 months. Non-compliance with this rule was frequently observed, in particular by external service providers who sometimes failed to do so even when instructed.

A number of **other matters** are regularly reported in the evaluations. Information provided to the public on the visa application procedures on consulates' and external service providers' websites is often unclear, incomplete or not user-friendly. There is confusion between the invalidation of visa stickers and annulment and revocation of issued visas. Practices not having a legal basis in the Visa Code, such as return control, administrative procedures under national law that delay processing as well as local alert lists, have been reported in various evaluations. In some cases, the handling of blank visa stickers was not always sufficiently secured. Full tracking for the distribution of visa stickers to local staff in charge of printing them, either in the IT system or at least on paper was sometimes lacking.

2.3. Points of particular interest

In many instances, experts were able to identify points of particular interest, including: e.g. well-drafted country assessments of migratory risk that summarise the socio-economic situation in the country, particular risk profiles and regions; summary records of the supporting documents and all investigations in the IT system; the constant presence of local consular staff at the external service providers to interview applicants; the deployment of experts in charge of detecting cases of fraud, including fraudulent travel or supporting documents to consulates; and providing applicants with a document giving grounds for refusal in greater detail, in addition to the standard refusal form and IT systems developed in coherence with the Visa Information System, following the workflow of the Visa Code and Visa Information System Regulation.

2.4. Conclusion

Based on the 29 evaluations carried out in relation to common visa policy, it can be concluded that Member States to a large extent adequately implement the common visa policy with decisions that, overall, are well justified on whether visas should be issued or refused. Serious deficiencies were identified recently in two Member States[14].

Despite a common regulatory framework, Member States' visa-issuing practices still diverge in several aspects. Consular staff sometimes still view Schengen visas as 'national' visas. Competition between States in 'attractive markets' as well as 'visa-shopping' weakens the perception of Schengen as a common travel area.

However, a substantial number of the deficiencies identified have been successfully addressed in these past five years. The Visa Code amendments that became applicable in 2020 seek to address several of these issues and strengthen the harmonised implementation of the common visa policy by providing faster and clearer procedures for legitimate travellers. The changes are based to a large extent on the findings of Schengen evaluations. For instance, for issuing multiple-entry visas with long validity as well as more technical aspects, some findings have also led to practical guidance in the form of Visa Code handbooks.

3. RETURN

3.1. Introduction

A fair and efficient system to return illegally staying third-country nationals is an essential component of a well-functioning European asylum and migration management system.

The Return Directive[15] is the **main legislative act** governing return, which sets the common standards and procedures for an effective and fair return of illegally staying third-country nationals. The Directive leaves significant flexibility to the Member States as to the concrete measures to be taken at national level to implement it, resulting in different systems and approaches being taken by Member States.

The Return Directive is a 'hybrid instrument', as it applies both to cases of presence on the territory of a Member State of a third-country national who does not fulfil, or no longer fulfils the conditions of entry as set out in the Schengen Borders Code, and to cases in which other conditions for entry, stay or residence in that Member State are not complied with. To the extent that it applies to third-country nationals who do not fulfil or who no longer fulfil the conditions of entry in accordance with the Schengen Borders Code, the Return Directive constitutes a development of the provisions of the Schengen *acquis*[16].

This is why the new Schengen Evaluation and Monitoring Mechanism introduced evaluations also in the field of return to ensure that the rules of the Return Directive are correctly

---

14 In 2019, the unannounced evaluation of the **Netherlands** (in Rabat, Morocco), a serious deficiency was identified for non-compliance with the 2-week deadline for giving appointment to lodge Schengen visa applications, due to the length of the existence of the problem and the length of the waiting time, which made it impossible to get an appointment to request for a visa. In 2018, **Finland**, serious deficiencies emerged as regard first the overly dependence on the external service provider, which even owned and managed the visa application database goes beyond the role assigned to the external service provider by the Visa Code and raised serious data protection concerns. Second, no supporting documents for applications were required from Russian citizens during the time of the evaluation.

15 Directive 2008/115/EC, OJ L 348, 24.12.2008, p. 98.

16 See recitals 25-30.

implemented by the Member States[17].

To bring more measurable results in returning irregular migrants, the Commission adopted, on 2 March 2017, a Recommendation on making returns more effective when implementing the Return Directive[18]. This Recommendation provides guidance on how the Return Directive should be applied to achieve more effective return procedures, in particular by fully exploiting the flexibility provided by the Directive.

Between 2015 and 2019, evaluation visits were carried out in the 26 countries of the Schengen area as well as in Croatia. In addition, four unannounced evaluations took place, two of which were in the same country.

3.2. Recurrent deficiencies or areas for improvement

One of the main cross-cutting issues observed during the evaluations is the general **lack of reliable and comparable data** on returns-related aspects. In the absence of an Entry/Exit System, limited data on overstayers are available, and several Member States do not have updated and complete data on key aspects of the return procedure. Moreover, there are differences from one Member State to another on the criteria considered for the collection of data, as some of them include for instance returns enforced under the Dublin Regulation (which are outside the scope of the evaluations for returns) and others no. This situation negatively affects the possibility to assess the situation and therefore the effectiveness of the national return systems in the Member States. However, the amendment to the Migration Statistics Regulation[19] and the entry into operation of the Schengen Information System for return[20] will contribute addressing this issue.

A major aspect of the return system is the **systematic issuing of return decisions** as soon as an illegal stay is detected, either when an illegal stay follows the termination of a legal stay (e.g. asylum, residence permit, visa) or otherwise, as required by the Return Directive. Differing practices have been observed in this area. In some Member States, a return decision can be issued even in the absence of the individual concerned; in others, they are regularly issued only upon apprehension/re-apprehension. Another Member State issues a return decision as soon as the asylum application is rejected at first instance and before the deadline for lodging an appeal against such decision expires. A recent judgment of the Court of Justice of the EU[21] clarified that in this case the legal effects of the return decisions are however suspended for as long as the asylum applicant has a right to remain pending the outcome of the appeal against that rejection.

---

17 All Member States are bound by the Return Directive, with the exception of Ireland by virtue of Protocol 19 on the Schengen *acquis* integrated in the framework of the European Union and Protocol 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaties. To the extent that the Directive applies to third-country nationals who do not fulfil or who no longer fulfil the conditions of entry in accordance with the Schengen Borders Code, Denmark takes part to it by virtue of Article 4 of Protocol 22 annexed to the Treaties and Iceland, Norway, Switzerland and Liechtenstein are bound by it based on the respective agreements associating them with the implementation, application and development of the Schengen *acquis*.

18 C(2017) 1600.

19 Regulation (EU) 2020/851, OJ L 198, 22.6.2020, p. 1, amending Regulation (EC) 862/2007, OJ L 199, 31.7.2007, p. 23.

20 Regulation (EU) 2018/1860, OJ L 312, 7.12.2018, p. 1.

21 Judgment of the Court of Justice of 19 June 2018, C-181/16, *Gnandi*, EU:C:2018:465.

In several Member States, return decisions issued to illegally staying third-country nationals only establish the obligation to leave the Member State concerned and does not clearly state that they should leave the Schengen area as a whole. The absence of the European dimension in return decisions can lead to unauthorised secondary movements. Moreover, there is a widespread lack of a system for ensuring that return decisions, and entry bans where necessary, can be issued when the illegal stay is discovered during an exit check. Some Member States do not consider that this may be appropriate in certain circumstances to prevent future re-entry and reduce the risks of illegal immigration, following a case-by-case assessment.

Inadequacies exist with regard to issuing of **entry bans** to third-country nationals illegally staying in the EU. In particular, those who have not complied with an obligation to return within the period for voluntary departure are not always issued an entry ban, as required by the Return Directive, therefore limiting the deterrent effect of entry bans. The Return Directive leaves wide discretion to the Member States on the length of the entry ban, which should in principle not exceed five years. The evaluations indicated major differences on the maximum length of the ban allowed under national law and in the way the duration of entry bans were determined. Moreover, the time limit of an entry ban must start running from the date of departure, to ensure that its duration is not unduly reduced.[22] Shortcomings were observed on this point as in some Member States entry bans enter into force from the date of its issuance.

On **voluntary return assistance**, evaluations showed that there is scope for improving the support provided to irregular migrants willing to depart voluntarily, notably by ensuring that the assisted voluntary return and reintegration programmes have a wider scope (e.g. not limited only to rejected asylum seekers or third-country nationals lost a right to stay in the EU).

Several Member States do not take sufficient measures to ensure the **enforcement of return decisions**. Once issued, there are no suitable mechanisms in place to ensure the systematic monitoring and to follow-up on these measures to ensure that decisions are enforced. A recurrent problem is that national authorities do not hold sufficient data on the national return situation and there are no active case management systems or measures to locate returnees or to prevent them from absconding. This is also exacerbated in few cases by the lack of assisted voluntary return programmes as well as the lack of measures to deal with last-minute subsequent asylum applications or medical claims.

The approach towards **unaccompanied minors** is different among Member States. The identification of durable solutions, looking at all available options, including return to the country of origin and reunification with family members in a third country, is an essential component of the best interests of the child determination, which however is not carried out by all Member States. This results in 'return' not being assessed as a possibility when conducting the individual assessment of the best interests of the child. As a consequence, unaccompanied minors may face situations of legal uncertainty about their status and are not returned even when this might be in their own interest. This practice can also create unintended consequences for irregular migration of unaccompanied minors.

In several Member States, the national law either does not define the elements that substantiate the existence of a **risk of absconding** or defines it in an unclear or too restrictive way. This has a major impact on assessing individual cases to set the period for voluntary

[22] Judgment of the Court of Justice of 26 July 2017, C-225/16, *Ouhrami*, ECLI:EU:C:2017:590.

departure and for the need to apply restrictive measures such as detention, negatively affecting the intended effects of the Return Directive.

To enforce return decisions, **detention** can be used as a legitimate measure of last resort for as short a period as possible and as long as removal arrangements are in progress and executed with due diligence. In some Member States, ineffective rules on detention contribute to an increase in the risk of absconding, affecting the functioning of the return system as a whole. In particular, some Member States do not use the flexibility provided by the Return Directive and they have a maximum length of detention in their national law significantly below the maximum length period allowed under the Directive, which is not always enough to prepare and enforce returns. Moreover, the limited availability of places in pre-removal detention centres in some Member States also contributes to the ineffectiveness of the system.

Furthermore, material conditions of detention centres are not fully harmonised among Member States. In few Member States, specific concerns exist regarding a lack of adequate privacy of detainees, sufficient information on the rights and obligations of the detainees, and a prison environment of the detention centres which does not fully reflect the administrative nature of the deprivation of liberty. In addition, in several Member States detention does not always take place in specialised detention centres and the separation requirement from prisoners is not always fully applied.

Not all Member States have in place an effective **forced-return monitoring system**. In several Member States, the human and financial resources available, the scope for monitoring and the number of operations monitored are very limited. This situation can also have a negative impact on the monitoring of forced-return activities carried out by the European Border and Coast Guard Agency.

3.3. Points of particular interest

During the evaluations, examples of measures taken by Member States to strengthen the return system and to better assist illegally staying third-country nationals were identified. For instance, the practices of providing a written translation of the main elements of the return decision into a language the third-country national can understand, and the involvement of 'cultural mediators' at the different stages of the immigration procedures proved to be particularly useful both in providing support to the police and in helping the third-country nationals to better communicate and fully understand the implications of the return decisions.

Setting up a last-minute asylum procedure that enables any relevant application to be evaluated without postponing or delaying the removal of a third-country national, or assessing whether the application is admissible, can be considered as a good practice. It increases the effectiveness of the forced return operation while ensuring the respect of the principle of *non-refoulement*.

In one Member State, the adoption of return, removal and entry ban decisions in a single step proved to reduce the administrative burden while respecting the procedural rights of the returnees.

The regular online publication of forced-return monitoring reports, including in English, as part of the national Ombudsman annual general report is a useful practice followed in a Member State to ensure further scrutiny over the removal process, to enhance its transparency and to further support the effectiveness of the forced-return monitoring mechanism.

3.4. Conclusion

Based on the 31 evaluations carried out in relation to return, it can be concluded that the return systems of the Member States are in general compliant with the Return Directive. No serious deficiencies have been identified**.** However, in some Member States practical and normative obstacles exist which negatively affect the effective enforcement of returns. Although Member States have in several cases made progress in implementing the recommendations addressed to them, the implementation of recommendations has been slow.

Since 2015, the EU and some Member States have been facing particular challenges in dealing with returns, due to the high number of third-country nationals that entered irregularly the Schengen area. With an unprecedented number of asylum applications since 2015, some Member States have been overburdened in dealing with these applications. In those Member States, the structural weaknesses of their national return system have been exposed and, in some cases exacerbated.

In 2018, the Commission tabled a proposal for a recast Return Directive[23], which consists of **targeted amendments aimed at maximising the effectiveness of the EU return policy** while safeguarding the fundamental rights of irregular migrants and ensuring the respect of the principle of *non-refoulement*. The proposed recast relies on the information collected during the evaluations and addresses several of the aforementioned shortcomings, such as setting an obligation for Member States to establish assisted voluntary return programmes and introducing a common list of objective criteria to determine the existence of a risk of absconding. Furthermore, the amended proposal for a Regulation establishing a common procedure for international protection[24] requires that a return decision is immediately issued to an asylum seeker whose application is rejected[25].

4. POLICE COOPERATION

4.1. Introduction

The 1990 Schengen Convention introduced provisions to increase cooperation and information exchange between the police forces of the Member States as a compensatory measure to the abolition of internal border controls. The provisions concern cooperation to prevent and detect crime, operational cooperation, e.g. the possibility to extend surveillance or to continue pursuing criminals across internal borders (‘hot pursuit’), and exchange information for the prevention and repression of crime or threats to public order and public safety.

The Schengen police cooperation *acquis* gives flexibility to the Member States in the way to implement it. A major part of the Schengen police cooperation framework is based on Council non-binding acts such as good practices (‘Schengen catalogue) and guidelines[26] as well as the core provisions of the Schengen Convention that are mainly implemented through bilateral or multilateral agreements concluded by the Member States.

---

23 COM(2018) 634.

24 COM(2020) 611.

25 See recital (31a) and Article 35a.

26 See for example Single Points of Contact (SPOC) Guidelines (Council Doc. 10492/14, 13 June 2014), Police and Customs Cooperation Centres (PCCC) Guidelines (Council Doc. 9105/11, 18 April 2011); Manuals on law enforcement information exchange (Council Doc. 6261/17, 4 July 2017) and on cross-border operations (Council Doc. 105050/4/09, 14 December 2009) or Compendium on law enforcement liaison officers (Council Doc. 11996/14, 5 September2014).

In addition, the police cooperation legislative framework remains fragmented. Since 1990, the EU framework on information exchange and data access for law enforcement purpose has continuously evolved. While a part of it does not formally belong to the Schengen *acquis*, it is closely linked to it. For this reason, the implementation of the Prüm Decisions, the Europol Regulation and other non-Schengen legal instruments have been taken into account during the evaluations. This contributes to assessing how Member States cope with general information exchange requirements provided by the Schengen Convention.

Between 2015 and 2019, evaluation visits were carried out in the 26 countries of the Schengen area as well as in Croatia.

4.2. Recurrent deficiencies and areas for improvements

Law enforcement **information exchange** is the area of the police cooperation *acquis* where non-compliant findings were identified in several Member States. Most of these findings related to providing access to the Visa Information System to their police and other law enforcement agencies under the conditions laid down in the Council Decision[27].

The **Single Point of Contact** (SPOC) – as the national 'one-stop shop' for international law enforcement cooperation gathering under the same management structure all main international law enforcement communication channels – is a key tool in this area. However the evaluations highlighted recurrent and at times very significant margins for improvement, notably: providing SPOC direct access to all relevant national databases (Customs and Border Guards included); setting-up an interoperable case management system for the SPOC and all law enforcement agencies; deploying automated data loader; providing SPOC sufficient access to translation services; deploying tools for tracking legally binding deadlines; improving staff knowledge of the guidelines on the choice of communication channels and of relevant foreign languages. Additionally, a few SPOCs still do not operate SIENA (Europol Secure Information Network Application) or Interpol channels 24/7. Eventually, in a number of SPOCs, the lack of user-friendliness of the interface to access the relevant national law enforcement databases hinders the performance.

While access to the Schengen Information System (SIS) and the other EU[28] and International[29] communication channels and databases is established, solutions allowing to search simultaneously all these databases with a single query are not always in place (most notably for wanted persons). In addition, police officers have often very limited access rights to make full use of the different databases and their awareness about those was also found limited/ lacking. Furthermore, in most Member States, the mobile access to the databases for street-level police officers is insufficient.

Other necessary improvements concerned: insufficient use of Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States (so-called Swedish initiative); the uneven implementation of Article 45 of the Schengen Convention requiring registration forms to be forwarded to law enforcement authorities for rented accommodation, such as hotel rooms; the limited information available on the actual use in police work of Article 46 of the Schengen

---

27 Council Decision 2008/633/JHA, OJ L 218, 13.8.2008, p. 129.

28 See for example Europol Information System (EIS) and Secure Information Exchange Network Application (SIENA).

29 See for example Interpol Nominals, Stolen Motor Vehicles (SMV), Stolen and Lost Travel Documents (STLD) databases and I-24/7, i.e. network enabling investigators to access Interpol's range of criminal databases.

Convention (and Article 7 of the Swedish initiative) on spontaneous transmission of information by a Member State to another.

Tactical police radio communications between Member States were rarely found operational. Many police forces operating in border areas beyond the reach of their national radio coverage resort to non-secure radio communication tools or mobile phones to contact their counterparts for a background check, with a risk of communication failure, misunderstandings or undue delays in case of alerts for discrete checks.

Strategic crime threat assessment and risk analysis is another area where the evaluations highlighted the need for most improvements[30]. The evaluations showed that crime threat assessments and risk analyses, when they exist, often remain confined to the remit of the specific law enforcement agencies producing them. Such clustering prevents developing a genuine national picture of the crime threat and risks, and prevents sharing information with the other Member States to better inform a joint response to cross-border crime.

Many of the **bilateral and multilateral agreements** concluded between neighbouring Member States were found to be either outdated, underused, raising unaddressed implementation issues or at times, suffering from an excessive time span between signature, ratification and implementation. In addition, the proliferation of bi/tri/multilateral agreements has created a complex web of arrangements based on the principle of reciprocity. This is particularly true for smaller and landlocked Member States where police officers conducting cross-border operations have to observe two, three or four different sets of rules depending on the Member States they go through during the day. Therefore, the level of law enforcement cooperation that is taking place between different Member States varies - sometimes greatly – across the EU, affecting as a result both the nature and quality of cross-border police cooperation.

The evaluations also recurrently identified the need to improve **training and awareness** among police staff on police cooperation and information exchange channels and instruments. Joint training between relevant national law enforcement agencies (including customs) and with neighbouring Member States on the use of cooperation tools is insufficiently developed. Life-long learning and specialised training (including in relevant foreign languages), notably for the staff dealing with international police cooperation (e.g. the SPOC staff), were found in general weaker than the initial training. E-learning content is not always well established. Even when readily accessible, online training remains underused by police officers.

Operational cross-border cooperation was often found to be hindered by limitations imposed in the declarations or bilateral agreements regulating it. Very strict geographic, material or time scope limits are imposed by some Member States. Some imposed additional rules discouraging the practice of 'hot pursuits'. On cross-border surveillance, some heavy procedural conditions and/or additional restrictions are imposed on Schengen foreign police officers. Joint patrols and joint operations are often found to be insufficiently based on joint or at least shared risk analysis.

The 59 **Police and Customs Cooperation Centres** (PCCC) set up across the Schengen area are mostly located at Schengen internal borders. Police and most often customs and/or border guards from two, and up to four, Member States are collocated in these centres. They

[30] The lack of strategic analysis is among the gaps identified in the Commission Recommendation of 12.5.2017 on proportionate police checks and police cooperation in the Schengen area (C(2017) 3349 final of 12.05.2017).

contribute to the channelling of a large part of the law enforcement information exchange in the EU, essentially related to petty and moderately serious crime, illegal migration flows and public order. However, the evaluations found in many cases that the case management systems in use at the PCCCs (when existing) were not inter-connected nor connected with the ones used by the central authorities (firstly SPOC). Often secure and interoperable channels of communication were also found lacking. In addition, some PCCCs engage too often in so-called 'chain requests'[31]. Such practice is slowing down information exchange and represents a risk on information integrity.

4.3. Points of particular interest

Some bilateral and multilateral agreements enable to go much further than the Schengen standards for cross-border operations. They extend the scope – geographically, time-wise or materially (beyond the extraditable offences) – of cross border surveillance, 'hot pursuits', or joint patrols as well as the powers recognised to Schengen foreign police officers engaged in such operations (right to stop, question and apprehend offenders in Schengen foreign territory).

A very active decentralised operational cooperation was found at play in some border regions with practices such as joint operations planning, mutual deployments and exchange of equipment as well as joint teams or 'micro teams' preparing and carrying out locally targeted joint operations (e.g. against property crime). Regular joint training on cross-border operations practised by some neighbouring Member States highly contributes to this.

Some Police and Customs Cooperation Centres (PCCC) deliver regular analytical reports on cross-border crime to all partner law enforcement agencies operating in a given internal border region. Beyond, in a few occurrences the PCCC 'historic model' has evolved to become a genuine joint police station able to gain coherence and speed in dealing cases of serious itinerant and cross-border crime.

The decentralised roll-out and multiplication of access points to secure communication channels for police information exchange such as the Europol Secure Information Network Application (SIENA) and the use of automatic data loaders at the SPOC have also proven, where implemented, to provide significant efficiency gain.

The pooling of police liaison officers deployed to third countries between several Member States to ensure a wider international coverage at a reasonable cost is another good practice spotted by the past cycle of evaluations.

4.4. Conclusion

Based on the 27 evaluations carried out in relation to police cooperation, it can be concluded that Member States are generally compliant with the Schengen *acquis* in the field of police cooperation. No serious deficiencies were identified and only a few non-compliant findings were made, mainly in the area of information exchange and especially access to the Visa Information System for law enforcement purposes. However, recurrent issues prevent reaching the full potential of some of the existing police cooperation and information exchange tools.

In general, the Member States were keen to implement the recommendations but the implementation of some recommendations was slow, in particular those with significant

[31] Practice where an information request is channelled through from one centre to the next, until it reaches its final recipient.

budgetary impact e.g. setting up an automated data loader to the Europol Information System, improving or developing interoperable case management systems, or those requiring organisational changes for the police forces or in the Schengen State law enforcement inter-service coordination (e.g. setting up the SPOC took generally longer to implement).

In addition, the evaluations highlighted the need to consolidate the fragmented police cooperation *acquis* including, where necessary, by enhancing it for some of its elements that have become outdated considering the new operational requirements and technical developments of the past 20/30 years.

5. SCHENGEN INFORMATION SYSTEM

5.1. Introduction

The Schengen Information System (SIS) is the most widely used and largest information sharing system for security and external border management in Europe. The Schengen Information System is a key compensatory measure for the abolition of internal border controls as it offers essential support to security across the Schengen area.

SIS is a large-scale, centralised IT system that that enables competent national authorities, such as the police and border guards, to enter and consult different categories of alerts on persons and objects, for example, alerts on third-country nationals for refusal of entry or stay, persons wanted for arrest, missing persons, persons sought to assist with a judicial procedure, lost or stolen objects, among others. It also supports checks at the external borders, and law enforcement and judicial cooperation across Europe.

Its scope is defined in three legal instruments concerning border control cooperation, law enforcement cooperation and cooperation on vehicle registration[32]. The second generation of SIS became operational on 9 April 2013 in 28 Member States and at present already 30 Member States are connected to it[33]. On 28 November 2018, the European Parliament and the Council adopted a new legislative package that further widens the scope and functionalities of SIS to be implemented in three phases by 2021.

Each country using SIS is responsible for setting up, operating and maintaining its national system and designating a national 'SIRENE Bureau', in charge of ensuring the exchange of all supplementary information related to SIS alerts. The EU Agency for large-scale IT systems (eu-LISA) is responsible for the operational management of the central system and the communication infrastructure.

From 2015 to 2019, evaluation were carried out in the 26 countries of the Schengen area as well as Croatia and the United Kingdom, including 4 revisits and 1 unannounced evaluation.

5.2. Recurrent deficiencies and areas for improvement

One of the recurring deficiencies in implementing the Schengen Information System concerns **entering all the relevant information to SIS alerts**. It was found that authorities in many Member States do not always attach fingerprints and photographs to SIS alerts, even if these data are available at country level. This is mainly due to the lack of technical tools for

---

[32] Regulation (EC) No 1987/2006, OJ L 381, 28.12.2006, p. 4; Council Decision 2007/533/JHA, OJ L 205, 7.8.2007, p. 63, and Regulation (EC) No 1986/2006, OJ L 381, 28.12.2006, p. 1.

[33] In addition to the 26 countries of the Schengen area, the United Kingdom, Bulgaria, Romania and Croatia are connected to SIS. Yet, certain restrictions apply to the United Kingdom and Croatia regarding the use of Schengen-wide SIS alerts for the purposes of refusing entry into or stay in the Schengen area.

inserting or sending fingerprints and photographs as well as due to the lack of procedures at country level requiring authorities issuing the alert to add these data when available.

Another recurrent finding concerns the shortcomings in implementing some of the **functionalities introduced in 2013 by the second generation of SIS**, in particular, that not all information included in SIS alerts is displayed to the end-users. In some Member States, photographs, links between alerts, information on the type of offence, action to be taken, warning markers, or information on misused identity are not displayed at all or are not displayed appropriately. As a result, end-users are not provided with the most comprehensive information concerning the SIS alert and might have difficulties in identifying the individual that is the subject of the alert. In addition, in some Member States, new categories of alerts introduced by the second generation of SIS are not fully implemented and displayed to the end-users. However, progress in addressing these shortcomings has been observed during the last years.

Overall, the trend for **using SIS** has steadily risen. In 2019, it was searched more than 6.6 bn times; it stored more than 91 million alerts and achieved 283,713 hits.

In some Member States, however, the vehicle registration services still do not have access to SIS. This makes it impossible for them to verify if a vehicle that is presented to them for registration is reported stolen.

In few Member States, SIS is not always searched automatically when the national police system is searched, but it requires an additional action by the end-user. Although this is not the case in most Member States, in certain end-user applications SIS is not searched automatically, but only via a separate search. Since an integrated search in national databases and SIS allows an EU-wide real-time information exchange on crime and terrorism, those Member States were recommended to rectify this deficiency without delay.

In a limited number of cases, it was found that SIS checks were not systematically used in relation to the country's own citizens or residents, which in most of the cases was due to a lack of thorough knowledge of the purpose and scope of SIS among its end users.

In many Member States, the use of SIS by customs is still very limited and not well integrated into their working procedures. In some cases, customs officers at the external border crossing points do not have direct access to the system. In addition, the lack of specific training prevents integrating SIS-searches into their daily work of these Member States.

Most Member States perform checks against SIS on individuals crossing the external border in a satisfactory manner. However, some did not systematically carry out checks in the system at the time of the evaluation contrary to the requirements set out in the Schengen Borders Code[34].

In some Member States, travellers were systematically brought to the second line checks in the event of a hit on discrete check alert at the external border, which might have jeopardised the discrete nature of such check. The Member States where these findings were identified already took measures to cease these practices.

In terms of **technical implementation**, one of the most frequently recurring findings is that many Member States did not fully implement all search combinations provided in the SIS Central system and are unable to carry out complex queries. Some Member States are using only exact match searches in end-user applications due to which individuals presenting

[34] Article 8(2) and (3) Schengen Border Code.

themselves under a slightly modified name will not be found in the system. This might prevent the end-users from finding individuals and objects that have been flagged in the system.

Other issues regularly observed in the Member States include the lack of sufficient business continuity measures and the absence of the required security documentation for the national SIS. In certain cases, it was also found that the availability of SIS or the availability of the national applications used for SIS searches at the external border crossing points was not adequately ensured. Lengthy periods of unavailability of the systems on several occasions resulted in a relaxation of the external border controls and lack of checks contrary to the Schengen Borders Code.

Data quality is another issue in some Member States. Under the Schengen Information System legislation, it is the Member States that are responsible for the quality of the data uploaded into the system. On this basis, Member States are required to establish an effective mechanism at national level for data quality controls. However, the implementation of a quality control mechanism is not the case everywhere. Under the new Schengen Information System regulations, eu-LISA supports the Member States in this task with data quality checks and reports.

The **SIRENE Bureaux** are at the very heart of SIS operation and play a key role in effective information exchange. However, there are several persistent problems in almost all Member States related to the SIRENE Bureaux. The SIRENE Bureaux do not always have sufficient personnel and technical resources, including automated and integrated workflow tools, to enable them to exchange this information effectively. Despite the significant growth in SIS transactions the number of SIRENE operators was not increased and the extensive use of the system often brings the SIRENE Bureaux on the limits of their capacity.

However, in all of the Member States, the SIRENE operators demonstrated an exceptionally good knowledge of the SIS procedures. It can be concluded that the SIRENE Bureaux are in all Member States real centres of excellence in terms of the systems processes.

The handling of hit reported by the officers working in the field to the SIRENE Bureau was identified as a challenge in some Member States. In this regard, the Member States were encouraged to use standardised procedures and hit-reporting templates. Many Member States have now implemented such procedures and hit reporting forms. In many Member States hit reporting forms can be accessed via the end-user applications and can be sent directly to the SIRENE Bureau.

In almost all the Member States there is room for improvement in providing **training to the end-users**. Although there are training modules on Schengen and SIS, in many of the academies and other institutions that prepare the officers, an overall lack of follow-up training was observed in many Member States. As a result, due to the lack of training the required action, alerts were not always performed effectively. In particular, the lack of knowledge about the use of the search applications, and the use and meaning of misused identity information and links were the most common among the Member States.

The number of alerts on discrete and specific check aimed at tackling **terrorist suspects**, in particular foreign terrorist fighters, has been growing steadily in recent years, including the alerts inserted by Member States' state security services.

Moreover, most Member States had implemented the new measures available in the SIS to fight against terrorism, such as the immediate reporting procedure from the ground to the alert issuing country and the marker showing that the individual is involved in terrorism.

Some Member States put in place a very efficient procedure where if a possible hit on a discrete or specific alert for which immediate reporting is required, the SIRENE Bureau receives an instant notification and contacts by telephone the officer who launched the query. This ensures an immediate follow-up of the case.

The main challenge in this field is that the available measures are not always used in a consistent way across the Member States involved. There is also a lack of training on the new measures available in the system to fight against terrorism in some of the Member States.

5.3. Points of particular interest

Despite areas where further improvement is needed, there are many positive examples of state-of-the-art technical implementation of SIS and well-integrated end-user applications in the Member States.

On including all available data in the SIS alerts, some Member States automatically add photographs and fingerprints when they are available in the national systems to the alerts. Such solutions ensure that all the relevant biometric data are added to the SIS alerts, when available.

Several Member States have successfully rolled-out the new Automated Fingerprint Identification System (AFIS) at country level. AFIS search function can identify an individual on the basis of their fingerprints. In one of the Member States, the fingerprint search functionality is rolled-out extensively and is available most police stations.

Over the years, the SIS query applications were made more user-friendly and better integrated into the working procedures of the end-users. Moreover, these applications are increasingly used on different mobile devices which provides for more systematic use of the system. In some Member States the roll-out of the mobiles devices used for SIS queries is very extensive.

Some Member States have implemented very effective tools to exchange Schengen Information System alert information. For example, by passing information about the SIS hit immediately from the first to the second line external border control or sending an instant notification to the SIRENE Bureau.

Overall, the level of automation of the tools used by the SIRENE Bureaux is constantly improving, with automatic distribution of cases, forms processed automatically against national databases or checks against the several databases being increasingly used by the Member States.

Many best practices on training have been also identified, in particular where the SIRENE Bureau is involved in the development of training material or where online SIS training modules are available and accompanied by compulsory testing for the participants.

5.4. Conclusion

Based on the 32 evaluations carried out in relation the Schengen Information System, it can be concluded that Member States and other concerned Member States have generally implemented and used SIS effectively and in a uniform manner.

Although serious deficiencies in the implementation of SIS were identified in four Member State[35], these Member States have been actively working on remedying the deficiencies. However, in one of the cases the situation has not improved.

Overall, the evaluations indicate that Member States comply with the Schengen *acquis* in relation to SIS. Despite a number of recurrent issues identified during the evaluations that should be addressed by the Member States to achieve a state-of-the-art implementation of SIS, it remains a very effective migration, security and law enforcement information exchange platform.

The evaluations carried out during the first Multiannual Evaluation Programme indicate that recommendations addressed to the concerned Member States in the previous cycle have been overall well implemented. All evaluated Member States are also actively working on remedying the deficiencies and are keen to learn from best practice identified in other Member States. The Commission is closely monitoring the implementation of the actions aimed at remedying the deficiencies in those cases where serious deficiencies have been identified. These serious deficiencies are being effectively addressed.

The results of the Schengen evaluations have been used by the Commission for further policy and legislative work. They constituted a solid basis for the Commission's overall evaluation of the SIS in 2016[36] and the subsequent new regulation strengthening SIS entered into force on 28 December 2018. Moreover, the Commission Recommendation on the Catalogue of Best Practices and Recommendations[37] has also been updated including best practice that was observed while Member States were implementing it. This document is used by Member States as a reference point for implementing best practice at national level.

---

35 Serious deficiencies emerged in the 2015 evaluation of **Belgium** in relation to the non-adoption of the legal procedures concerning SIS II, the absence of plans to update the SIS technical copy to include the new functionalities of SIS II and deadlines for the ongoing reorganisation of the Single Point of Contact (SPOC) and the move of the National SIS (N.SIS) backup. The 2016 evaluation of **France** identified serious deficiencies as regards the non-effective roll-out of SIS to the end-users and the unsatisfactory availability of the N.SIS and the chain of national SIS-query applications especially at the external border crossing points. The 2017 evaluation of **Spain** identified as serious deficiencies the absence of an enforced security policy for processing SIS data, the limited authority of the SIRENE Bureau, the limited information displayed in the applications, and the absence of active follow-up of their developments by the N.SIS Office as well as the non-standardised procedures for handling hits. The 2017 evaluation of the **United Kingdom** indicated that the serious deficiencies emerged already in the previous 2015 evaluation under the old mechanism were not addressed. Serious deficiencies include the selective approach to SIS data, the high number of copies of the SIS database and their synchronisation problems as well as the limited reciprocity concerning the execution of the actions requested by the alert issuing Member States and the technical constraints of the end-user IT applications. Re-visits were carried out in Belgium in 2016 and in France in 2019. It is considered that Belgium, France and Spain have addressed all serious deficiencies.

36 Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA (COM(2016) 880 final of 21.12.2016).

37 Commission Recommendation of 17.4.2018 establishing a catalogue of recommendations and best practices for the correct application of the second generation Schengen Information System (SIS II) and the exchange of supplementary information by the Member States competent authorities implementing and using SIS II and replacing the catalogue established by the recommendations of 16 December 2015 (C(2018) 2161 final of 17.4.2018).

6. DATA PROTECTION

6.1. Introduction

A further important part of the Schengen *acquis* are the rules on the protection of personal data. The data protection legal framework underwent a major reform in 2016, which notably aimed to strengthen the rights of individuals in the digital era. The General Data Protection Regulation (GDPR)[38] applicable since May 2018 and the Data Protection Law Enforcement Directive, which had to be transposed also by that date[39], are applicable also in this area.

The Data Protection Schengen Evaluations assess how Member States implement and apply the Schengen *acquis*, in particular on the Schengen Information System (SIS) and Visa Information System (VIS) against the background of the data protection requirements. This includes also the role of the Data Protection Authorities as regards the supervision of the authorities managing and using the SIS and the VIS as well as the management of requests and complaints by individuals.

Between 2015 and 2019, evaluation visits were carried out in the 26 countries of the Schengen area as well as in Croatia, Ireland and Cyprus.

6.2. Recurrent deficiencies and areas for improvement

Before the 2016 reforms, most Member States concerned had adopted adequate **legislation to transpose and implement the EU *acquis*** in this field. Following the adoption of the data protection reform, the latest evaluations identified in some Member States delays in transposing the Data Protection Law Enforcement Directive into national law and/or in implementing the General Data Protection Regulation[40] as well as in adapting the national SIS- and VIS-related legislation.

The **data protection supervisory authorities** (DPA) are the national bodies responsible for monitoring the compliance of the various actors with and for enforcing data protection law. EU law[41] requires that each DPA acts with complete independence in performing its tasks and exercising its powers.

Overall, this requirement has been implemented correctly in the Member States. However, in some cases, the evaluations indicated elements undermining the complete independence of those authorities. Some examples include the right of the government to dismiss the head of the DPA in situations other than serious misconduct; risk of influence of the government on the work of the DPA (e.g. right to supervision, entitlement to give instructions, directions, guidelines, mandatory additional and special tasks; involvement of the government in the work of the DPA e.g. by having a representative of the government in the DPA; involvement of government in selecting staff of the DPA); or DPA is not involved in the budget proposal. In some Member States, the DPA does not have full and independent discretion on the use of its budget. Some of those issues have been solved in the follow-up to the Schengen

38 Regulation (EU) 2016/679, OJ L 119, 4.5.2016, p.1.

39 Directive (EU) 2016/680, OJ L 119, 4.5.2016, p. 89.

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

41 Article 16 of the Treaty on the Functioning of the European Union, Article 8 of the Charter of Fundamental Rights of the European Union; Article 52 GDPR and Article 42 of Directive (EU) 2016/680.

evaluations and in the context of the reform of the national data protection legislation to implement the GDPR and transpose the Data Protection Law Enforcement Directive.

Some DPAs were found to lack sufficient **human and financial resources** to effectively carry out all their SIS- and VIS-related tasks. A recurrent problem is the limited number of IT experts working for the DPAs to assess the data protection related technical aspects of the systems. Staff numbers have often also not been sufficiently increased to cope with the additional tasks of the authorities under the new EU data protection rules.

In many Member States, more frequent and comprehensive inspections by the DPAs would be necessary in order for them to fulfil their tasks of monitoring the lawfulness of the processing of SIS and VIS personal data. In some Member States, the DPA is in regular informal contact with the SIS and VIS authorities in order to discuss data protection related aspects; however, more formal inspections and audits would be required. These inspections and audits should cover all the data protection aspects of the structure and the functioning of SISII and VIS, including the quality of the data entered into the systems. Regular checks on SISII and VIS files, including on the basis of log file analysis are necessary. In some Member States, the deadlines for carrying out the first audit of the data processing operations in the SIS and/or VIS system have not been met.

The evaluations indicated in general that the **data subjects' rights** in relation to SIS II and VIS data have been correctly dealt with. Only in some cases, there were concerns on the deadline for replying to data subjects' requests or that there was a restriction of access requests to once per year. In a number of Member States, the information to data subjects about the SIS II and VIS systems and the related data subjects' rights including on the appeal possibilities should be improved. This should be done by providing more detailed and accessible information (including to which authority a data subject request has to be addressed), and by providing this also in English as well as by providing model letters for making data subjects' requests for access, correction and deletion of data. The letters to the data subjects should also include information on the appeal possibilities and the right to send a complaint to the DPA. The websites of the SIS and VIS authorities should include links to the websites of the competent DPAs. Not all Member States provide templates or forms to request access, correction and deletion of data enabling the exercise of the data subject rights. The lack of proper information might constitute a constraint for the effective exercise of data subjects' rights.

The processing of personal data in the **Visa Information System (VIS)** was generally found compliant. However, some deficiencies were often observed in this respect. Most Member States had no regular pro-active self-auditing on data protection compliance by data controllers, including no regular review of logs. Automated tools for log control are rare. In few cases, deficiencies were identified on the accessibility of logs to data protection supervisory authorities and data controllers (e.g. logs on operations by the service providers or consulates). In few Member States, data, and in particular logs, are kept for periods not in line with the VIS Regulation because they were deleted too soon (possibly hampering supervision) or, more frequently, kept for too long if not indefinitely. Not all Member States implemented the automatic deletion of data.

In some Member States, evaluations highlighted a lack of clarity on the tasks and allocation of responsibilities for the processing of personal data among different authorities involved in the visa-issuing procedure and processing of related data. In particular, for Schengen visas issued at the external borders, it is sometimes unclear who the data controller is.

All Member States apply comprehensive physical, organisational and IT security measures for VIS data. Most Member States have adopted the required security plan. Improvements might also be appropriate in certain cases such as a more complex password policy, encryption of passwords, or regular revision of the access authorisations/user profiles.

Data protection officers, who are designated by the data controller with the task to ensure compliance with data protection provisions should often be more closely involved in overseeing the processing of personal data in the Schengen context.

Member States are generally ensuring appropriate contractual guarantees for the security and confidentiality of data when using external service providers in the visa application process. Such contracts also ensure that external service providers are supervised by the consulates. In a few cases, however, deficiencies were observed for the secure transfer of data from subcontractors to consulates (lack of encryption), and for data storage by the external service providers (exceeding the retention periods defined in the Visa Code). In a few cases, evaluations also found that systematic controls of the activities of consulates and external service providers are carried out, including for compliance with data protection requirements.

In most Member States, the law enforcement authorities have access to VIS data for criminal investigation. However, in certain Member States evaluations found that the requirements for recording each access showing the exact purpose of the access and the reference to the national file were not sufficiently met. Also, the records kept are not frequently audited.

Some consulates keep local warning lists with data on persons who have been indicated as having a history of irregularities that may justify the refusal of a visa. Given that such processing of personal data cannot be based on the EU *acquis*, the Member States must ensure that the appropriate legal basis for such processing of data is provided under their national law[42].

Evaluation showed that Member States' authorities generally comply with the data protection principles while processing data in **Schengen Information System (SIS) data**. However, a number of areas require improvements.

In contrast to the VIS, the responsibility for processing personal data entered in SIS is usually well defined. It is clear which authority is responsible for the management and processing of data in the national Schengen Information System (data controller), which, very often, is the national police or the Ministry of the Interior. In some Member States, the data controllers do not ensure that other authorities with access to SISII data (end users of SISII, such as border guards or district police forces) apply appropriate security measures when processing SISII data.

Overall, the authorities managing the national SIS system (the data controllers) in all Member States apply comprehensive physical, organisational and IT security measures in respect to SIS data. However, some improvements were deemed necessary in relation to particular aspects, such as a more stringent password policy, encryption of passwords or backup copies, access to internet on SIRENE terminals, improvements as regards the physical access or in respect of the user profiles. In some cases, the recovery centre did not have full functions, such centre and /or backup storage was not in different locations. Often, shortcomings were identified on the authentication mechanism, at least for critical users such as SIRENE officials, therefore the implementation of a two-factor authentication system was deemed

42 This issue is also mentioned in the Annex on Common Visa Policy, in the chapter 'Other matters'.

necessary. Some Member States have not adopted the required security plan, or the plans required improvements.

In many cases, a comprehensive and clear methodology or practice for frequent self-auditing of the effectiveness of security measures and the lawfulness of the data processing in by the data controller, including on basis of logs was lacking.

On logs, Member States are required to ensure that access to the Schengen Information System and operations are logged. However, in a few cases query logs are only stored in the applications used by authorities (other than data controller) accessing and processing SIS data (end users of SIS). Such data cannot always be accessed by the data controller, which was seen as a considerable weakness.

Few SIS data controllers provide periodical reviews of the audit log records. In most Member States, automated tools for auditing logs are not available, or the automated checks are very limited. In few cases, logs are retained for periods that do not comply with the prescribed deadlines.

The data protection officers should in some Member States be more closely involved in overseeing the processing of personal data in the Schengen specific context. With few notable exceptions, there was no regular and continuous training for all operational staff (police officers and civilian staff) specifically on data protection and data security.

6.3. Points of particular interest

A number of measures have been observed as point of particular interests. Some DPAs are providing considerable resources for the consulting and supervisory work of the Schengen related system or invest a lot in the training of staff dealing with SIS and VIS matters. In some Member States the DPAs, SIS and/or VIS authorities provide very detailed and accessible information on the processing of personal data in SIS and VIS and the related data subjects rights. Some authorities that manage the VIS are frequently controlling the processing of personal data in consulates and in External Service Providers.

Some authorities that manage the SIS regularly monitor SIS operations by the end users, including on the basis of log controls and make a log control by the responsible officer a pre-condition for the renewal of the authorisation of staff to access the system. Further, in some Member States, a regular training is provided to staff of authorities having access to SIS II and VIS data, including on data protection and data security.

6.4. Conclusion

Based on the 29 evaluations carried out in relation to data protection, it can be concluded that Member States generally implement and apply the relevant provisions on the SIS and the VIS in compliance with data protection requirements.

However, a number of deficiencies and areas for improvements have been repeatedly identified in all Member States. The Member States are in general taking the necessary steps in order to follow-up on the findings and recommendations. While overall some progress has been made to address the deficiencies, implementing the recommendations has been slow. In several cases, even the recommendations of previous evaluations have not been fully implemented, in particular those linked with security and monitoring of the lawfulness of data processing.

PART II: STATISTICS

1. EVALUATIONS

Between 2015 and 2019[43], Member States were evaluated according to the Multiannual Evaluation Programme in all policy fields[44]. In addition, Ireland, Croatia, Cyprus as well as the UK were evaluated in all or selected policy fields (Table 1).

Under the SCH-EVAL regulation in addition to the programmed evaluations *ad-hoc* evaluations can be organised as *revisits* or *unannounced* evaluations. Evaluations of border controls at internal borders are performed only as unannounced visits. There is also the possibility to conduct *thematic evaluation* of the implementation of certain elements of the Schengen *acquis* across Member States. A total of 27 unannounced evaluations and 8 revisits as well as 2 thematic evaluations were carried out in addition to 164 announced evaluations in the reference period.

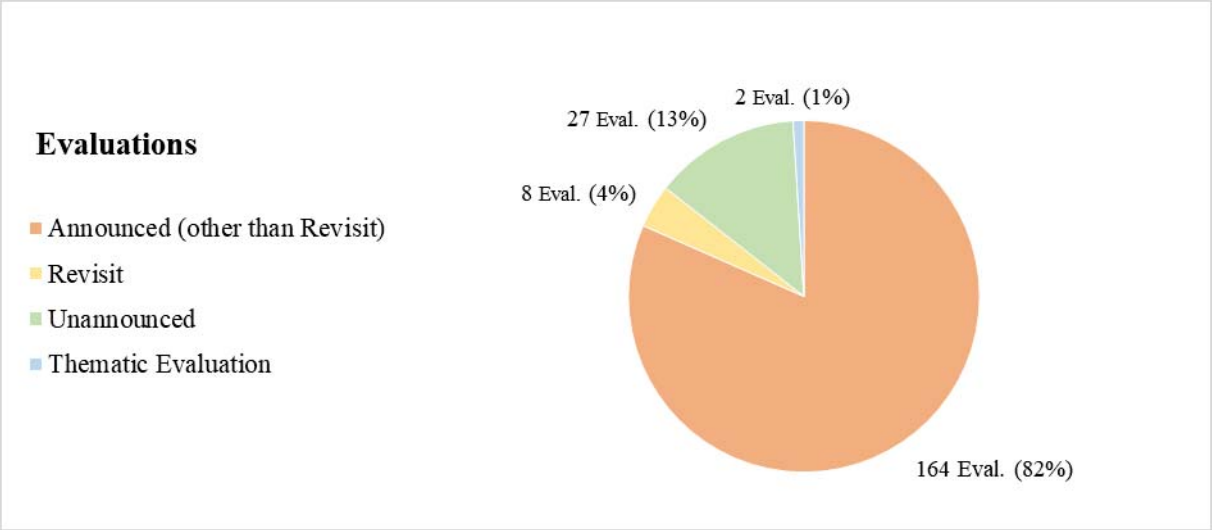
Evaluations are mostly based on a standard questionnaire and evaluation visits on-site. Rather exceptionally, it was made use of the possibility of questionnaires based evaluations[45]. A single evaluation visit was sufficient for evaluations policy fields other than external border management, where up to 3 evaluation visits may be necessary for the same country depending on the characteristics of the borders (Figure 2).

43 As the UK was still a Member State during the reference period, references to 'Member States' in Part II should be understood to include the UK unless explicitly stated otherwise.

44 Liechtenstein did not undergo evaluations in the fields of external border management and common visa policy.

45 On four occasions evaluations were based on stand-alone questionnaires, namely for the evaluation of Liechtenstein in the field of return (2015), Malta for SIS (2016), Croatia in relation to compliance with firearms legislation (2016) and Judicial cooperation in criminal matters (2017). Thematic evaluations were also questionnaire based.

Figure 2 – Evaluations by Type



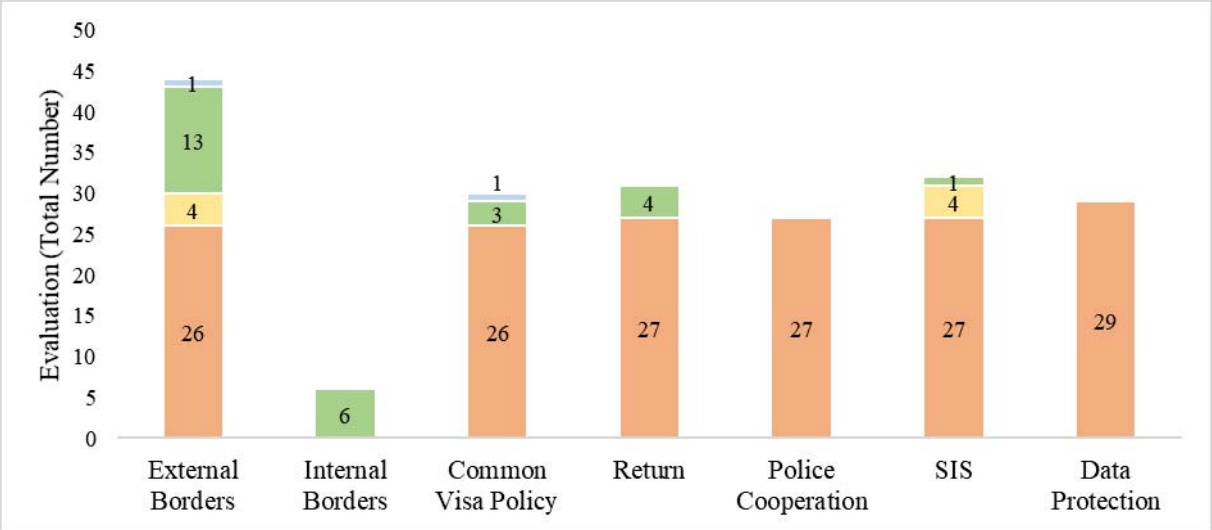


Table 1 – Evaluations carried out during the first Multiannual Evaluation Programme (2015-2019)

	2015	2016	2017	2018	2019
ANNOUNCED VISITS / QUESTIONNAIRES Unless otherwise specified, the evaluation covered the following policy fields: External Borders, Visa, Return, Police Cooperation, SIS and Data Protection	• Austria • Belgium • Germany • The Netherlands • Liechtenstein (Return, Police cooperation, SIS, Data Prot.)	• Luxembourg • Italy • Greece • Croatia (Ext. Borders, Visa, Return, Data Prot., Police Cooperation and Firearms) • Malta • France	• Croatia (SIS) • Denmark • Iceland • Sweden • Portugal • Spain • Norway	• Switzerland • Latvia • Finland • Estonia • Lithuania • Ireland (Data Prot.) • Croatia (Judicial Coop. in Criminal Matters)	• Czech Republic • Poland • Slovenia • Hungary • Slovakia • Cyprus (Data Prot.)
UNANNOUNCED VISITS	• Sweden (Ext. Borders) • Latvia (Int. Borders) • France, Germany (Int. Borders) • Spain (Ext. Borders) • Hungary (Ext. Borders) • Poland (Ext. Borders) • Greece (Ext. Borders) • Switzer. (Int. Borders)	• Denmark (Ext. Borders) • Spain (Ext. Borders) • France (Return) • Austria, Italy (Int. Borders) • Germany (Return) • Estonia (Ext. Borders)	• Czech Republic (Int. Borders) • The Netherlands (Visa) • Hungary (Return) • Poland (Ext. Borders) • Italy (Ext. Borders) • The Netherlands (Ext. Borders)	• Belgium (Visa) • France, Italy (Int. Borders) • Greece (Ext. Borders) • Germany (SIS)	• France (Ext. Borders) • Spain, France, the Netherlands and Switzerland (Visa) • Germany (Return)
REVISITS	• Poland (SIS)	• Belgium (SIS)	• UK (SIS) • Croatia (Ext. Borders)		• Croatia (Ext. Borders) • France (SIS) • Sweden (Ext. Borders) • Iceland (Ext. Borders)
THEMATIC EVALUATIONS	• Local Schengen Cooperation in New Delhi and Ankara (Visa)				• National strategies for European Integrated Border Management

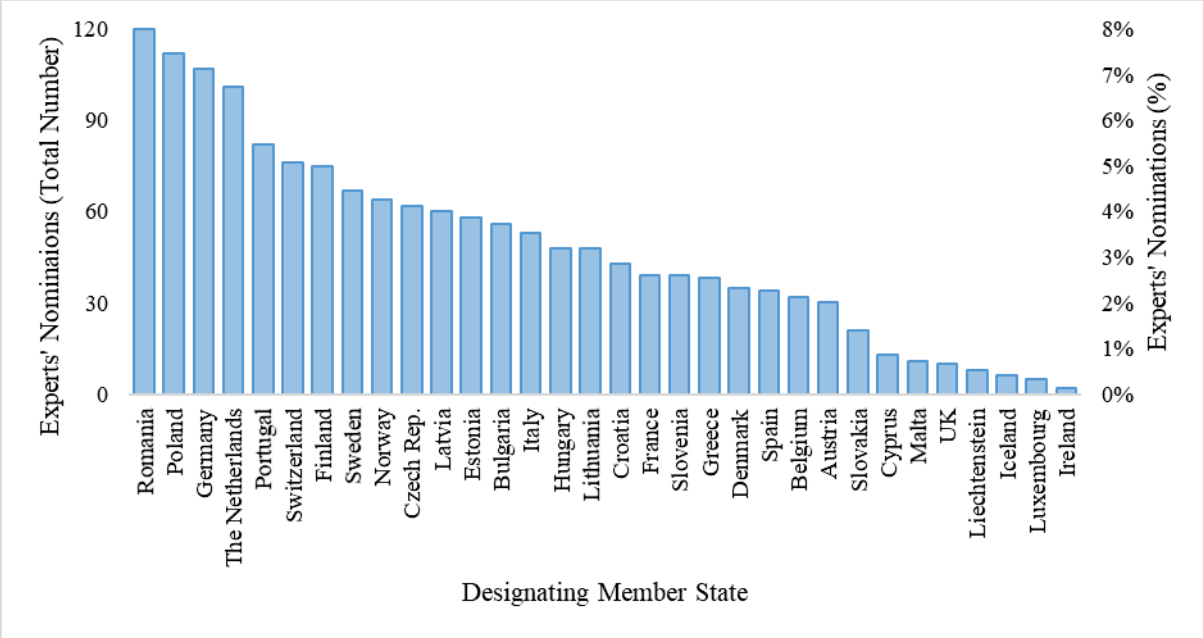
2. MEMBER STATES' EXPERTS

The effectiveness of the Schengen Evaluation and Monitoring Mechanism depends on the participation of highly qualified experts designated by the Member States. Their participation is also key to strengthen the trust among Member States and beneficial to spread the knowledge of the pertinent legal framework at national level[46].

The SCH-EVAL Regulation lays down the provisions for the participation of Member States' experts to the evaluation. Further to the invitation of the Commission, the Member States *shall* designate experts who are available for participation in the respective evaluation visits, indicating their area of expertise.

Over the first Multiannual Evaluation Programme, all 32 Member States contributed experts to the Schengen evaluations, however in very different proportions. One third of the over 1 500 nominations comprised experts from five Member States, namely Romania (7.7%), Poland (7.2%), Germany (6.9%), The Netherlands (6.5%) and Switzerland (4.9%) (Figure 3).

Figure 3 – Experts' Nominations per Member State



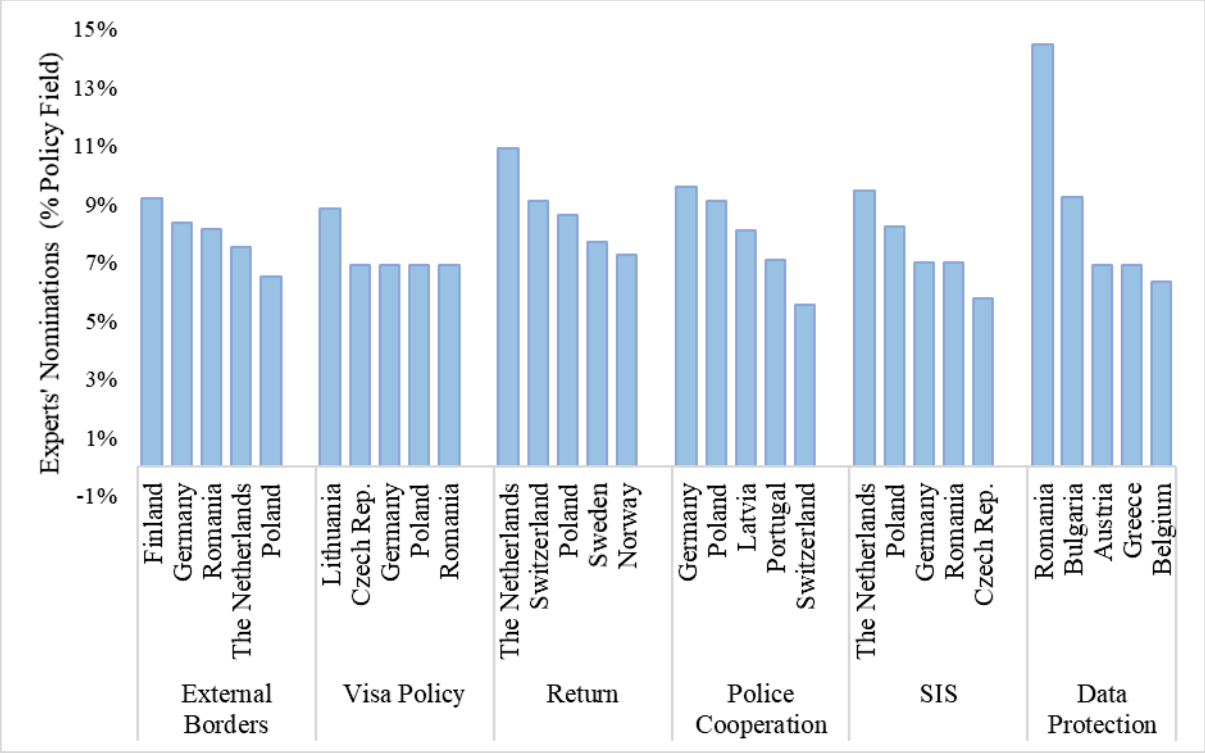
At policy field level, the contribution gap is even more remarkable as the top 5 designating Member States covered respectively between 36.5% (common visa policy) and 44% (data protection) of the nominations. Moreover, Member States showed different preferences so that the top five designating Member States varied depending on the policy fields (Figure 4).

Furthermore, overall 12 Member States did not contribute experts to at least one policy field completely, with five Member States designating experts only in three policy fields or less. In the policy fields of return and visa, seven Member States never designated any experts. The

[46] Ulrich/Nøkleberg/Gunghus, Schengen Evaluation – An Educational Experience (The Example of Norway), PHS Forskning 2020:1.

widest participation was recorded in the field of police cooperation and SIS, where nearly all Member States were represented over the reporting period[47].

Figure 4 – Experts' Nominations per Member State and Policy Field[48]

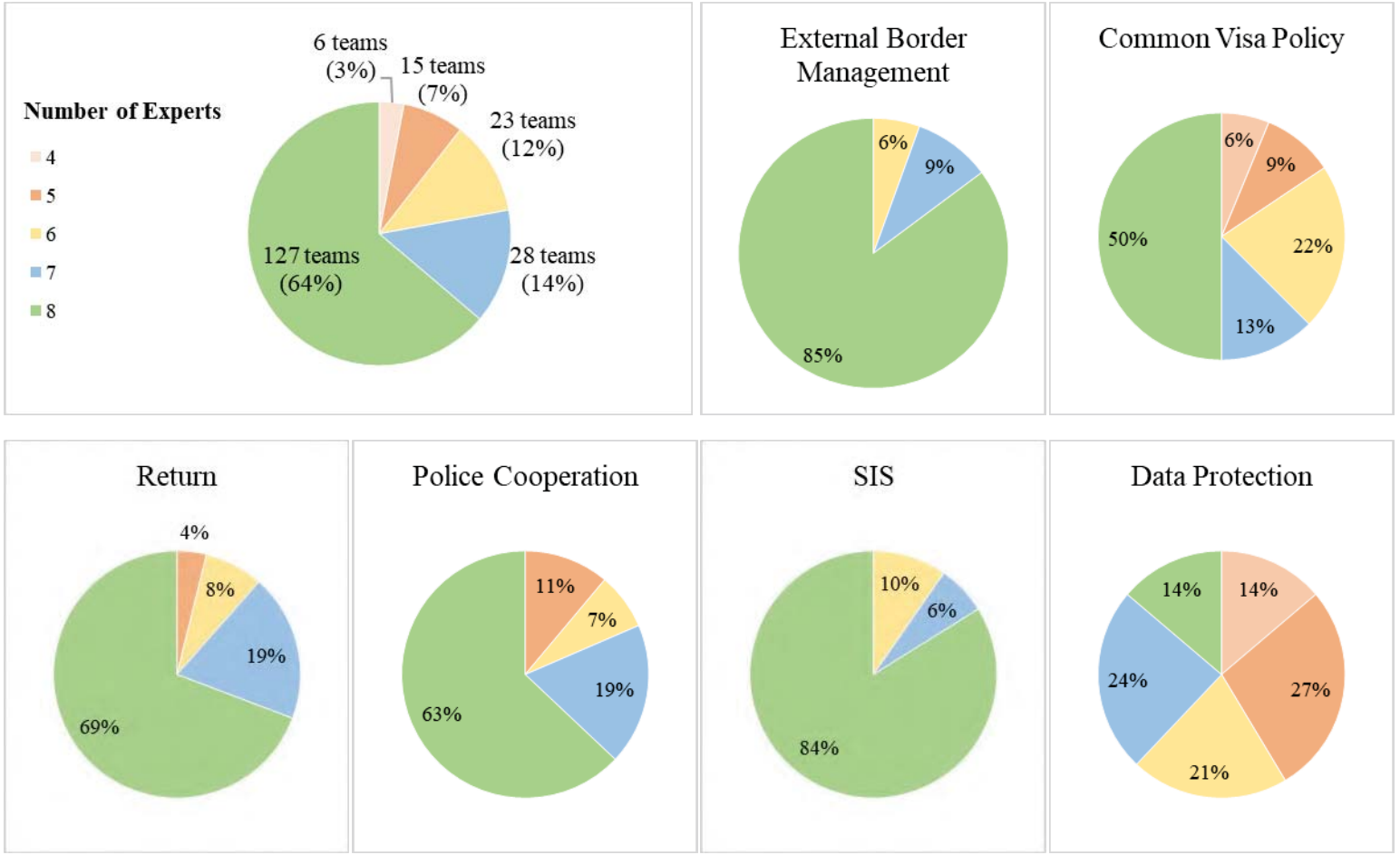


The maximum number of Member States' experts participating in an announced on-site visit is eight and six for an unannounced on-site visit. For announced evaluations the teams generally (127 (64%)) consisted of the maximum number of 8 experts and the number of designations was higher than 8, so that not all proposed experts could be retained. Yet on several occasions the time limit for the designation of expert was extended (occasionally even several times) due to a limited number of designations received and for 21 (10%) evaluations the number of experts was eventually below 6, hence critically low. The scarce availability of experts regarded in particular evaluations in the data protection field where 12 (out of 29) evaluation teams had fewer than 6 experts and only 4 teams included 8 experts. Occasionally a lack of experts affected also evaluations in the fields of common visa policy, police cooperation and return (Figure 5).

47 The number of countries of the nominated experts in the different fields were respectively: 28 (external borders), 25 (common visa policy), 25 (Return), 30 (police cooperation), 31 (SIS) and 28 (Data Protection).

48 Thematic evaluations are not included.

Figure 5 – Team Size – National Experts' Number in Announced Evaluations [49]



[49] Announced evaluations including revisits.

3. PROCEDURE LENGTH

The procedure under the Schengen Evaluation and Monitoring Mechanism is articulated into two main phases:

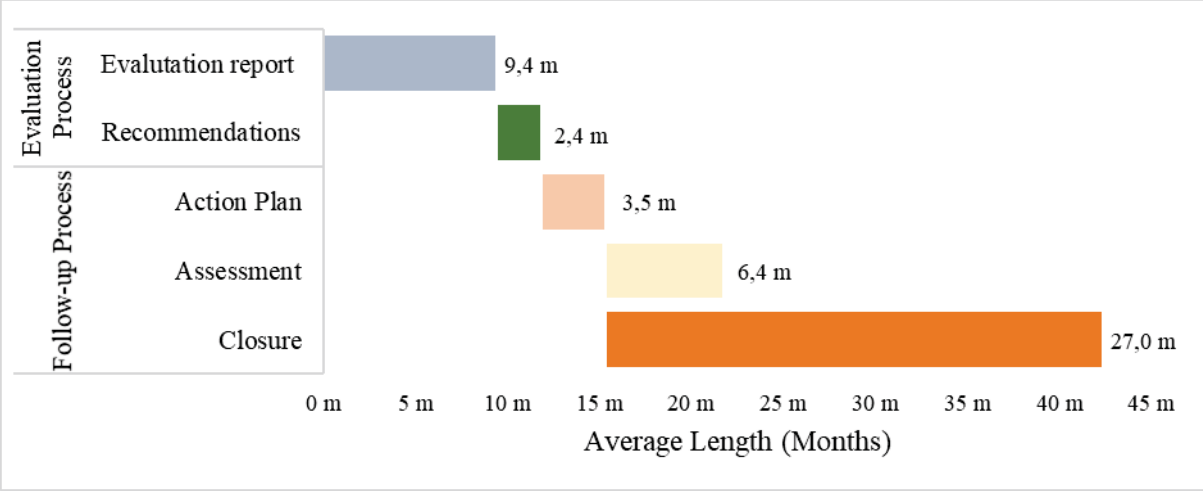
(1) the **evaluation process** to assess the implementation of the Schengen *acquis* which ends with the adoption of recommendations by the Council for the necessary action to remedy any deficiencies identified in the evaluation report adopted by the Commission; and

(2) the **follow-up process** aiming at the fulfilment of those recommendations to improve the implementation of the Schengen *acquis*.

Each phase includes a series of administrative measures and actions as well as implementing decisions. The SCH-EVAL Regulation shapes and regulates the key structure of the administrative procedure by defining the rights and responsibilities of all actors involved. Time limits are set only for certain intermediary steps, while a wide discretion is left to the actors involved in prioritising their tasks.

During the first Multiannual Evaluation Programme, the average length from the end of the evaluation visit or reception of the questionnaire (in case of a desk exercise) to the adoption of the recommendations by the Council was nearly one year (353 days), 9.4 months[50] (286 days) until adoption of the evaluation report by the Commission and 2.4 additional months (71 days) until the adoption of the recommendations by the Council. The average length of the follow-up phase, from the adoption of the recommendations until closure of the procedure, was 2.25 years (810 days) (Figure 6). Statistics on the application of the legal time limits and the length of the different phases are provided under the following sections.

Figure 6 – Length of the Main Procedural Steps



3.1. Legal Time Limits

3.1.1. Evaluation Process

Under the SCH-EVAL Regulation, time limits are indicated only for the transmission of the draft evaluation report to the Member State under evaluation (6 weeks) and the comments of

[50] The preparatory phase to organise evaluations starts in the summer of the preceding year with a standard questionnaire addressed at the same time to all Member States that will be evaluated.

the Member State on the draft report (2 weeks). It is estimated that the time limit of 6 weeks for the transmission of the evaluation report has been respected in 66% of cases. The average length of this procedural step was 44 days.

Only occasionally Member States requested an extension of the time limit for the submission of their **comments** for a due cause. The time limit was mostly extended in proximity of holiday period so to grant 10 working days to the Member States.

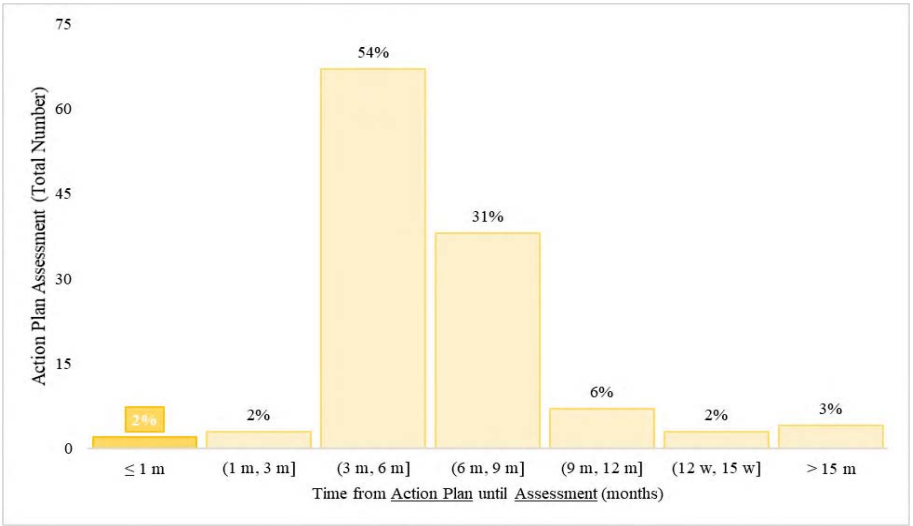
3.1.2. Follow-up Process

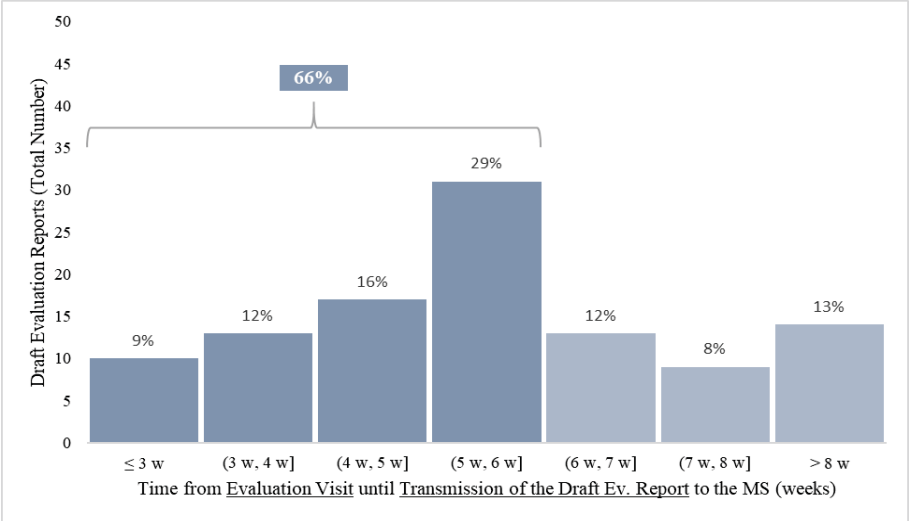
The SCH-EVAL Regulation set a time limit for the submission of the **action plan** by the Member State of 3 months after adoption of the recommendations reduced to 1 month where serious deficiencies emerged. In cases where the Member State was found to be compliant, but where the recommendations contain indications for possible further improvements, an assessment on a possible implementation of such indications is to be provided within six months. These time limits were met in the majority of cases. The average length for the submission by the action plan was 105 days and overly 63% of them were submitted within the respectively applicable time limit.

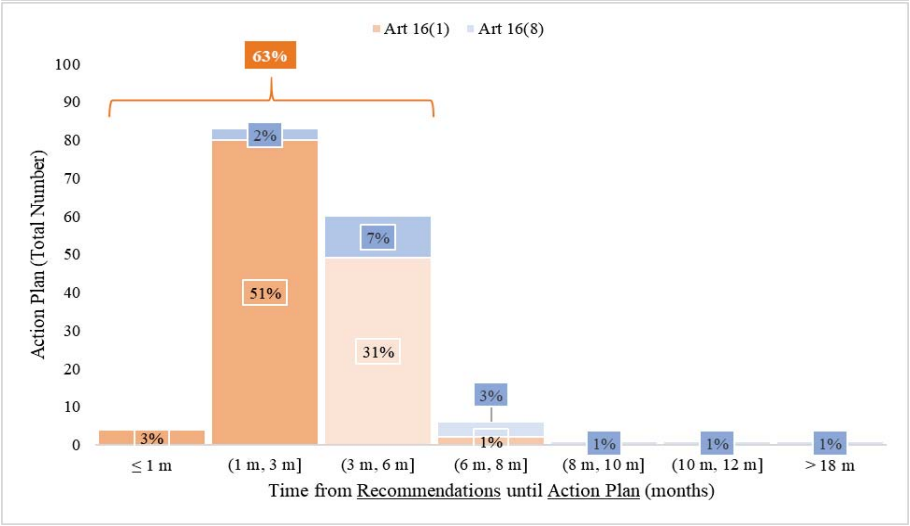
In cases where a Member State was not found compliant, the Commission is requested to present its **assessment** of the adequacy of the action plan to the Council within one month of receiving the action plan. This time limit is considered to be disproportionately short taken into consideration the procedural requirements to adopt a formal Commission communication and in particular the linguistic regime. The time limit could be met only for 2 evaluations where serious deficiencies had emerged and making use of the possibility of derogation from the normal procedure in case of an urgency situation. On average, the Commission adopted its communication in 196 days (6.4 months) from the reception of the action plan.

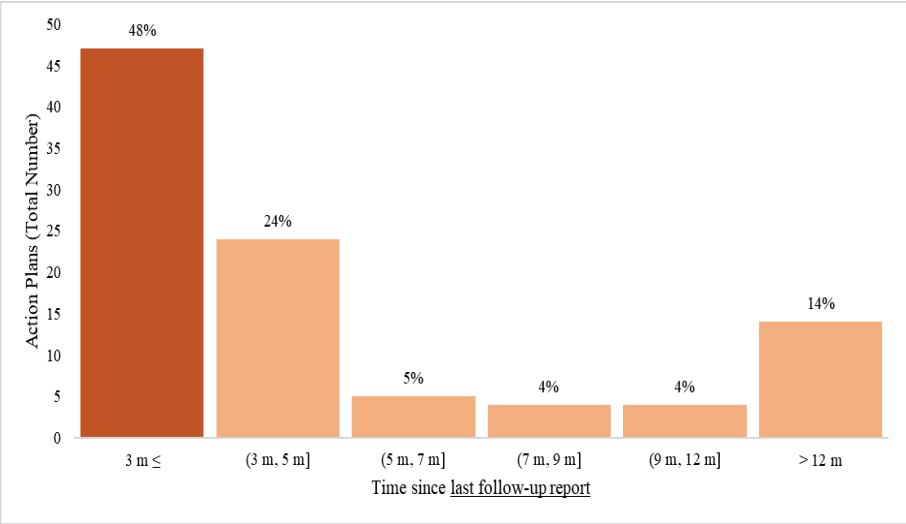
The SCH-EVAL Regulation requires the evaluated States to **report** on the **progress** made within six months from the submission of the action plan, or 3 months in cases where serious deficiencies emerged, and subsequently every three months in cases where Member States were not found fully compliant. This provision was not strictly applied. On 30/9, updated information had been provided since less than 3 months for half of the pending action plans for which reporting is still required. With very few exception information were provided on a regular basis even in cases of full-compliance.

Figure 7 – Legal Time Limits







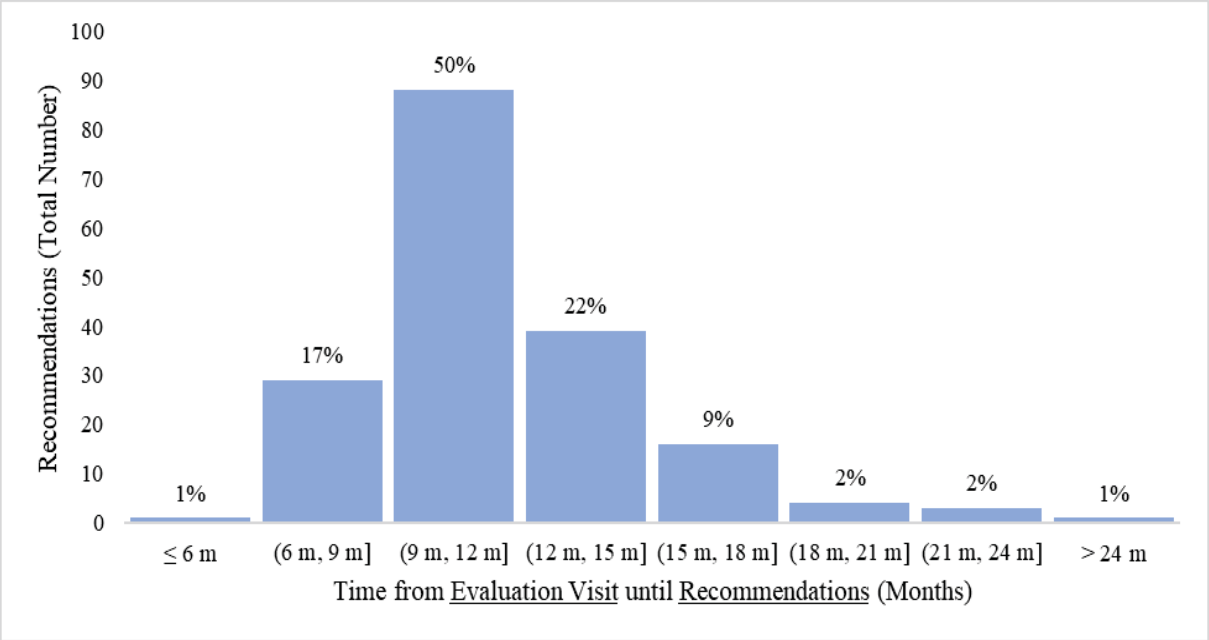


3.2. Length and variability of the process

3.2.1. Evaluation Process

The **yearly average length** of the evaluation process was **relatively stable** over the Multiannual Evaluation Programme[51], yet the **length of individual procedures** was very **variable,** ranging from 3 months to over 2 years. Most (85%) implementing decisions carrying recommendations were adopted between 6 and 15 months from the end of the evaluation visits (with a clear concentration around the average of 12 months) but in the remaining cases, it took up to 18 months, if no longer (Figure 8).

Figure 8 – Evaluation Process



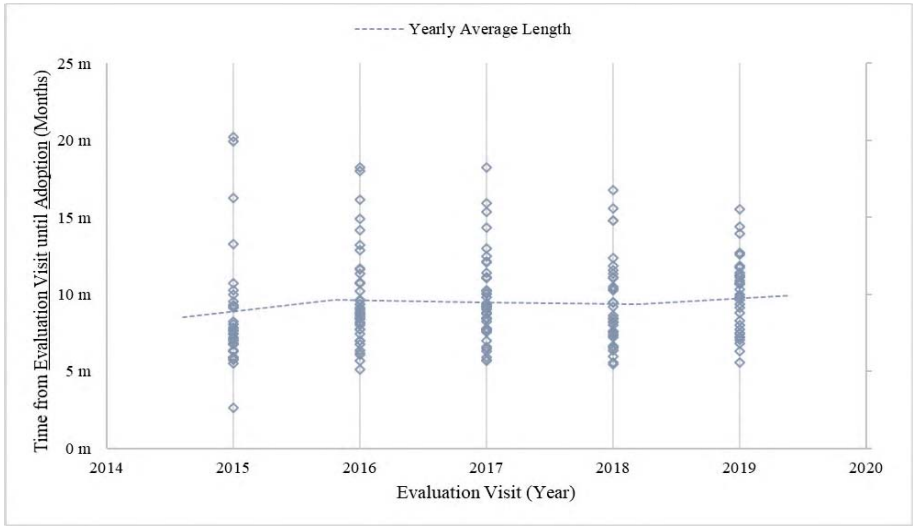
A **significant variability** characterised **all stages of the process**, but in particular the Council procedure. Most evaluation reports were adopted by the Commission in less than 9 months from the evaluation visit, while a restricted number of cases was significantly deviating from the average (Figure 9). The majority of the implementing decisions were adopted by the Council within 9 weeks from the Commission proposal, but over a third required over 12 weeks with a high relative dispersion[52] and no significant correlation with the length of the Commission procedure (Figure 10).

---

51 The average both for the adoption of the evaluation report by the Commission and of/for the recommendations by the Council were only slightly oscillating around the five-year average. Data for the referring to the 2019 evaluations are still incomplete and a certain distortion was caused by delays due to technical issues in connection with COVID19 related restrictions.

52 While in absolute terms the Commission procedure has a higher standard deviation than the Council procedure (respectively 93.1 p.p. and 56.72 p.p.), the relative standard deviation (RSD) for the Council procedure is more than twice higher (78.1 p.p. against 32.7 p.p.).

Figure 9 – Evaluation Reports



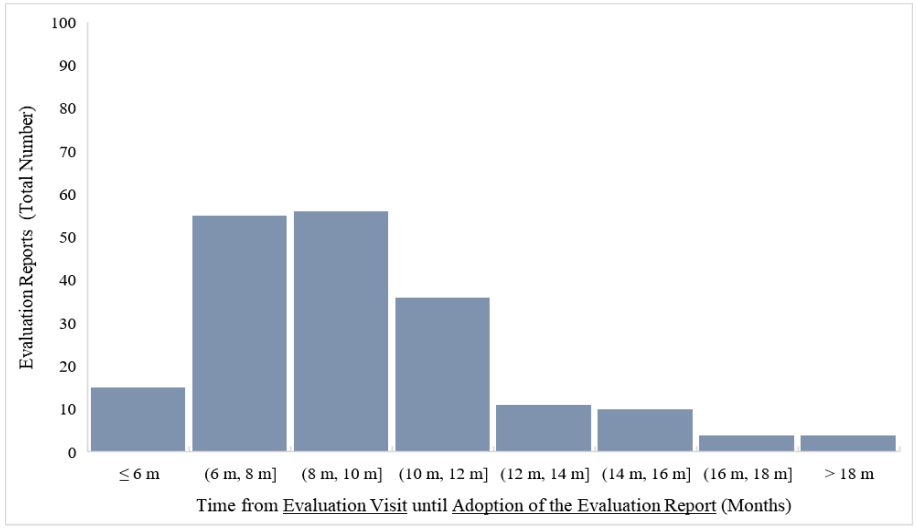
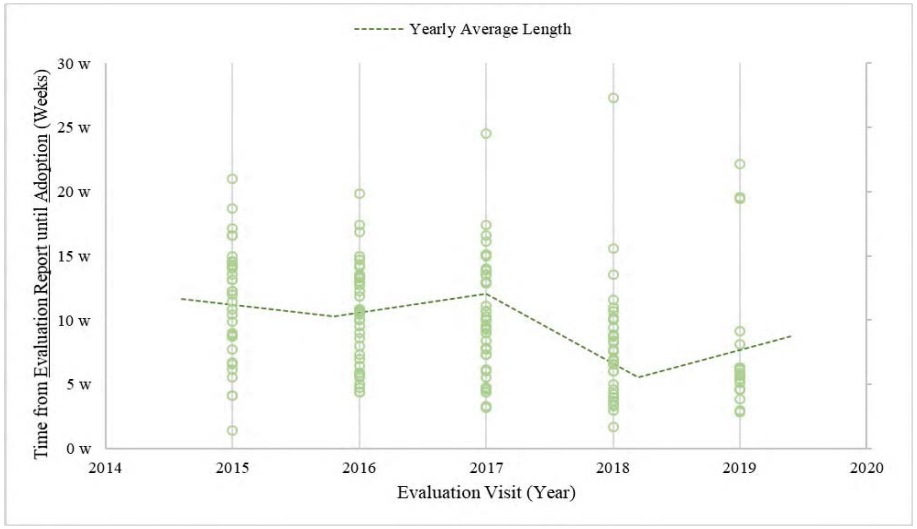
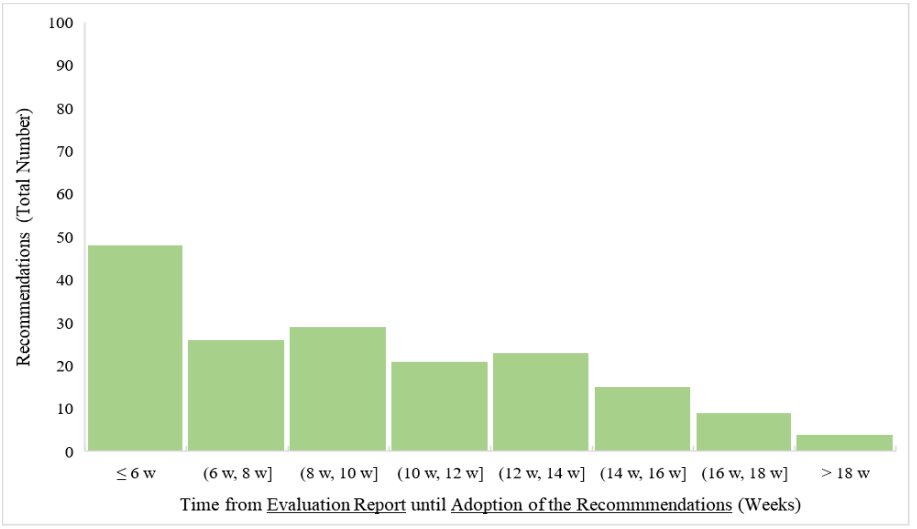


Figure 10 – Recommendations





3.2.2. Follow-up Process

While in a few cases the follow-up procedure was closed rather quickly, on average it took over 2 years until closure of the action plan from its submission. Given the significant number of action plans pending since over 810 days, 2 since over 3 years, it can be expected that at first the average might further increase. A certain distortion is however due to a number of procedures that have not been formally closed but *de facto* have been concluded or include few long -term actions to be taken (see below). In cases of non-compliant findings where legislative changes are necessary as a remedial actions, implementation, even if not contested, is bound to take very long. On the other hand, very technical recommendations related to either the administrative practice can often be implemented very fast.

Figure 11 – Formally Closed Procedures

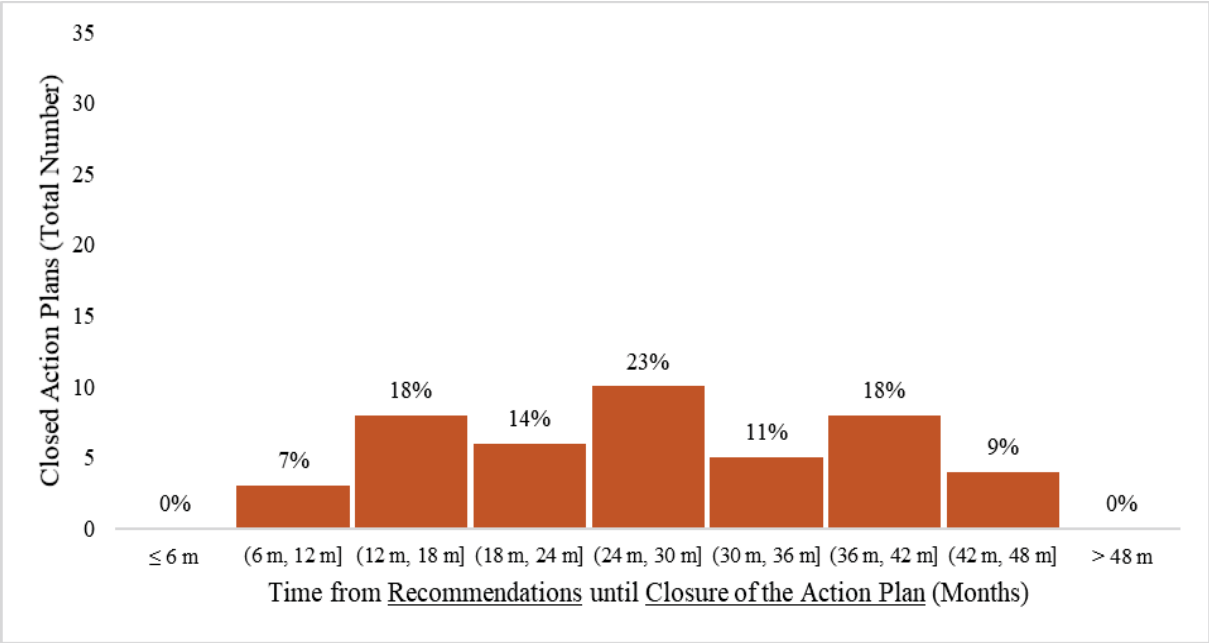
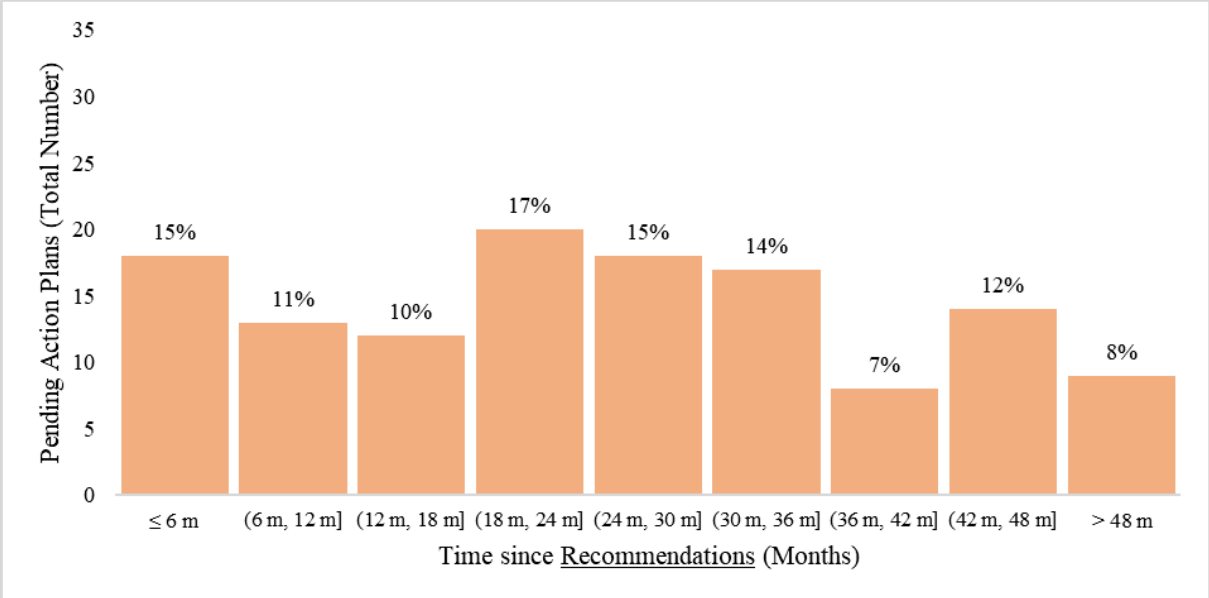


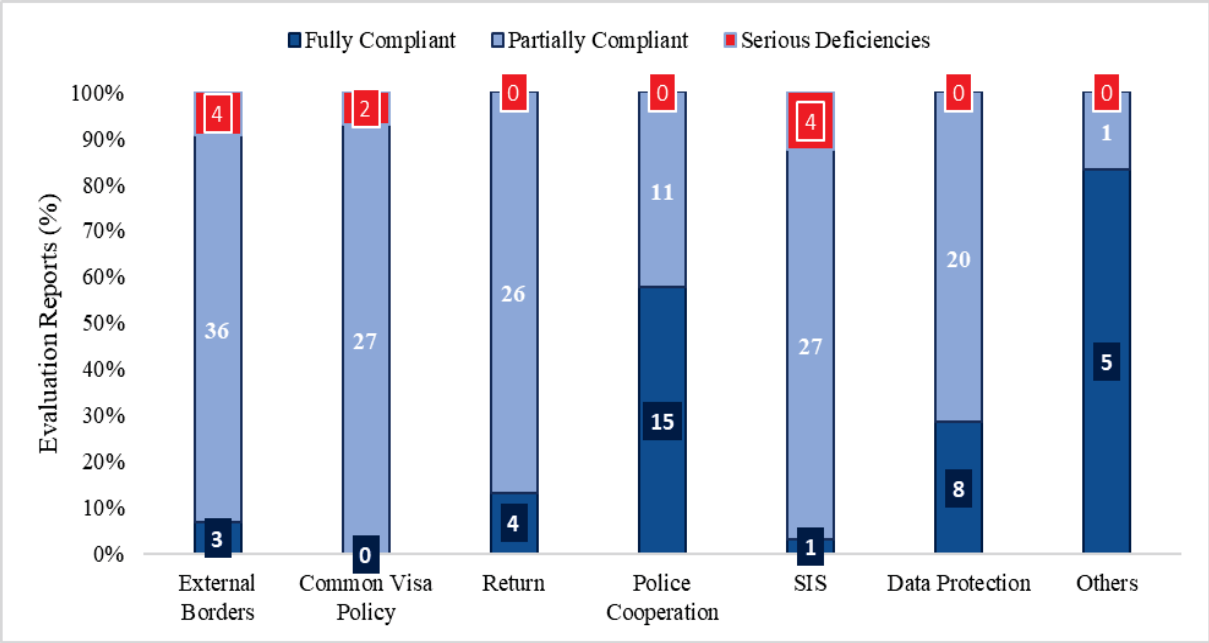
Figure 12 – Pending Action Plans



4. STATE OF SCHENGEN

On 5 November 2020, the Commission has adopted **198 evaluation reports** for evaluations carried out between 2015 and 2019. The adoption of a number of evaluation reports is pending. **76 %** of the evaluation reports adopted include '**non-compliant**' findings. Only in police cooperation and data protection, a significant number of Member States were found fully compliant but with improvement necessary. The number of non-compliant findings was generally quite small, if not negligible. **Serious deficiencies** were identified during **11 evaluations** respectively in the fields of external borders management (4), common visa policy (3) and SIS (4) **(**Figure 13**)**.

Figure 13 – Evaluation Findings [53]



With few exceptions, the evaluation reports were always accompanied by a proposal to the Council to adopt recommendations. The Council adopted **181 implementing decision.** A total of **4 605 recommendations** were made to the Member States; **34%** of those recommendations to be addressed with **priority**. More than half of the recommendations were formulated in the fields of external border management (35%) and common visa policy (25%). In the field of return (58%) recommendations were marked as priority while in common visa policy (37%), police cooperation (36%) and SIS (35%) over a third of the recommendations were marked as priority (Figure 14).

A total of **51 (**about **25%** of those where recommendations were already issued**)** evaluation procedures have been formally closed. In addition, few evaluations have been *de facto* discontinued as outstanding improvements will not be addressed or recommendations were absorbed in or overtaken by subsequent evaluation procedures.

A number of procedures are pending due to a few outstanding improvements that by nature cannot be implemented within a short time. In certain cases, older recommendations are still pending while the focus shifted from the old to a more recent action plan with more urgent recommendation or that *de facto* has absorbed the previous one even if the procedures have not been formally joined.

[53] Data do not include thematic evaluations.

Significant progress has been made with most action plans. Few more action plans are likely to be closed in the coming weeks and overall about 20% of the recommendations are still open (Figure 15)[54].

Figure 14 – Recommendations

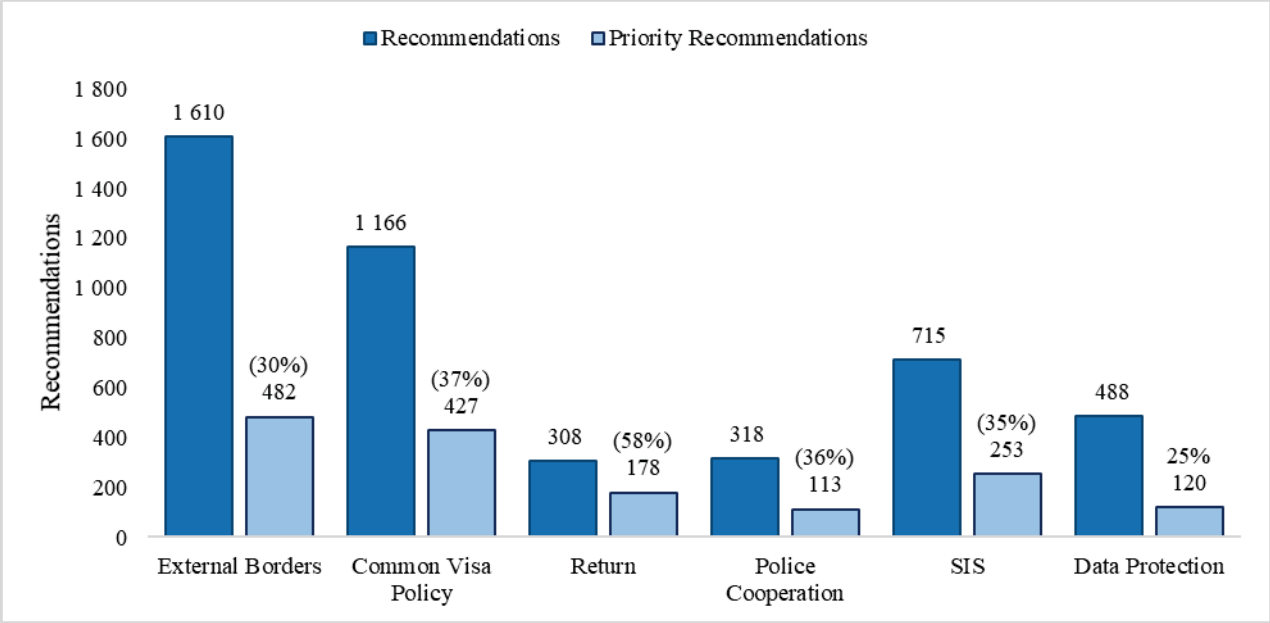
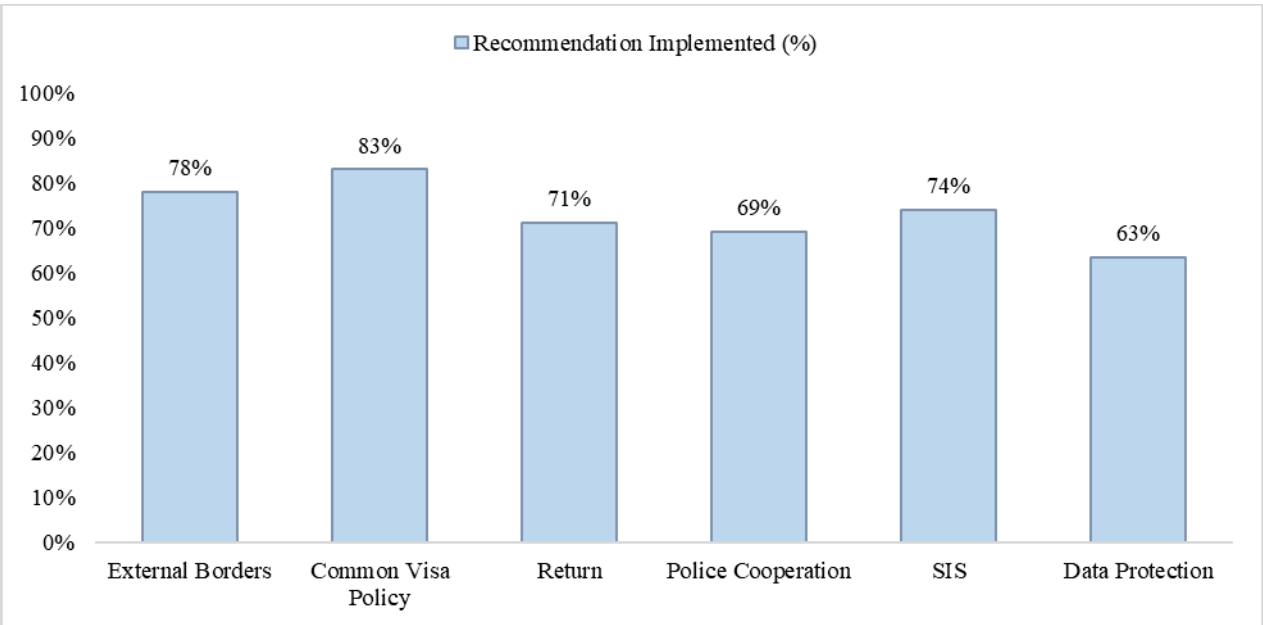


Figure 15 – State of Play of the Implementation of the Recommendations



[54] Data provide a best estimate based on the self-assessment of the concerned countries in the follow-up reports submitted until 5 November 2020.