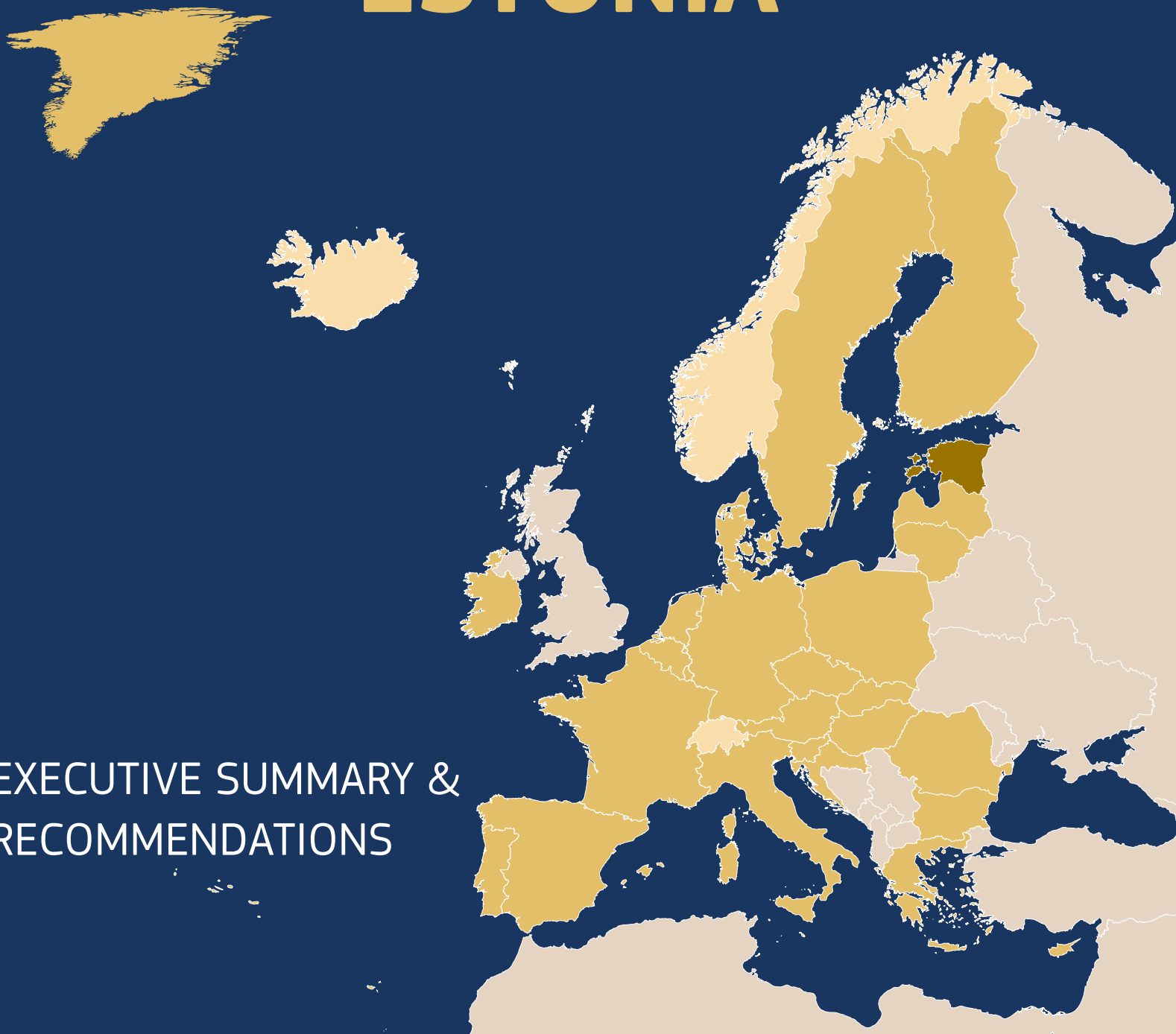
European Commission

Schengen Evaluation of **ESTONIA**



EXECUTIVE SUMMARY & RECOMMENDATIONS

SCHENGEN EVALUATION OF ESTONIA 2023

EXECUTIVE SUMMARY AND RECOMMENDATIONS

1. EXECUTIVE SUMMARY

A Schengen evaluation of Estonia was carried out between November – December 2023 by Commission and Member State experts accompanied by observers from relevant EU Agencies and bodies. It covered key areas of the Schengen acquis including external border management, absence of controls at the internal borders, return policy, police cooperation, the common visa policy, large scale information systems and data protection. Particular attention was paid to verifying the respect for fundamental rights. This activity results in the report of the 2023 Schengen evaluation of Estonia.

The war of Russia against Ukraine broke out in February 2022, starting a turbulent period for European security, which has an important impact on Estonia's implementation of the Schengen *acquis*, as the country is responsible for securing significant land and sea border sections with Russia. Hybrid challenges and evolving threats are the main elements to be addressed by the Estonian authorities responsible for the implementation of the Schengen *acquis*, in particular possible instrumentalisation of irregular migration from Russia to Estonia. This asks for constant readiness by the Estonian authorities and sufficient response capabilities. As a Baltic Sea state, the Estonian economy is highly dependent on adequate maritime traffic and on effective preparedness and response to maritime security challenges, including hybrid threats by Russia on critical infrastructure, which could have important cross-border security implications such as digital disruption. Several gas and oil pipelines and undersea cables run across the Baltic seabed connecting the Nordic region to the mainland. Given these threats, Estonia decided to legally empower the Navy to take over the sea border surveillance, with the exception of the law enforcement and the search and rescue activities that are still carried out by the Estonian Police and Border Guard Board.

Despite the complex environment, Estonia has maintained a **solid contribution to the functioning of the Schengen area**, in large part due to a strong implementation of **European integrated border management, based on a national strategy and inter-agency cooperation**. Estonia delivers a reliable contribution to the European Border and Coast Guard. Operational resilience and sufficient response capacity are ensured by efficient contingency and operational planning. **The national land border surveillance concept based on a comprehensive and efficient national database, combining all the relevant functionalities to support operational and tactical tasks is a best practice** as it ensures effective use of the resources and adequate operational response. The land border surveillance system functions effectively and it is under development to cover 100% of the land borders with technical equipment.

The national situational picture needs to be further enhanced as the National Coordination Centre does not operate efficiently to establish a comprehensive national situational picture, including operational and analysis layers, and to implement the legal requirements of the Schengen *acquis*.

The border checks at the land borders are adequate, although improvements are necessary in the production and use of tailored risk profiles and indicators, use of the automated border control and implementation of visa procedures. Moreover, the applications for querying the Schengen Information System are not used at their full potential due to insufficient training and knowledge of staff on their functionalities.

The level of human resources for border control tasks is at the minimum level and it is not efficiently adapted to the threat levels. The refresher and specialised training are not sufficient and not delivered regularly.

At the time of the visit, the Estonian authorities did not notify the Commission on the reintroduction of border control at any of the **internal border** sections.

Particular attention was paid to verifying the respect of fundamental rights with some challenges identified in the implementation and mainstreaming of certain fundamental rights safeguards, including in the context of training. Overall, the Estonian authorities duly consider fundamental rights when implementing the Schengen *acquis*. However, in the area of return, improvements are necessary in order to proactively consider risks of refoulement in each individual case, to systematically provide information on and ensure effective access to free legal aid and effective access to legal remedies, in particular during accelerated return procedures carried out within 48 hours of apprehension.

Estonia is **effectively implementing the Schengen *acquis*** in the field of **return**. The Estonian return system is well-organised with regard to the division of tasks of authorities involved, national strategies, contingency planning and the connected financial implications. A detention centre completed in 2018 offers good conditions for migrants awaiting removal, including regular medical visits, possibilities for leisure activities and consultation with return counsellors. However, the effectiveness of the forced-return monitoring system, could be improved by extending forced return notifications to those returns carried out within 48 hours and improving the transparency of the monitoring.

The set-up of a common IT system (*Illegaal2)* where procedural steps, decisions and further information related to illegally staying third-country nationals are indicated is considered a **best practice**. The system records all the information and documents of each individual subject to return, thus giving a complete picture of the situation of each third-country national.

As far as the implementation of the **EU visa *acquis*** is concerned, Estonia generally complies with the Visa Code and other relevant legislation in most essential aspects. No violation of key principles was observed. Visa applications at the consulate in New Delhi are examined in a satisfactory manner and decisions are reasonably well-founded. However, the team identified some deficiencies, including in relation to the monitoring of the external service provider, the verification of the admissibility requirements and the issuance of multiple-entry visas with long validity. Improvements are needed as regards the allocation of the responsibilities and tasks at the consulate and the consultation with the central authorities as well as regarding the supervision of the locally employed staff at the consulate.

Overall, the **Schengen Information System (SIS) and SIRENE** procedures are well integrated in border, migration and law enforcement processes in Estonia. However, further improvements should be made to ensure a more effective use of the SIS, in particular the implementation of all dactyloscopic searches in the SIS AFIS, all search functionalities of the SIS, the necessary additional human resources to be provided to SIRENE Bureau and the enhancement of the automation of the working processes, the timely and automatic insertion in SIS of alerts on missing persons (including minors), and the display of the results in the national applications used to query the SIS.

In the field of **police cooperation**, Estonia is in general implementing the Schengen *acquis* adequately. The Estonian internal security system is well structured and law enforcement cooperation is clearly regulated and implemented. The Estonian law enforcement system is adequately connected

to European law enforcement cooperation structures, including functional cooperation with Europol and involvement in EMPACT (European Multidisciplinary Platform Against Criminal Threats) activities. The national risk and threat assessment system has been systematically developed and harmonised with EU SOCTA (Serious and Organised Crime Threat Assessment). Estonia contributes actively to Europol's main strategic analytical products and law enforcement authorities are involved in EMPACT Operational Action Plans (OAPs). The overview of the national crime situation picture is well established at the strategic, operational and tactical level.

The well-established and comprehensive common annual planning system for **practical bilateral cross border cooperation** with Latvia and Information System POLIS-KAIRI were considered **as best practices**. However, there is **very limited capacity** to implement EU legislation, especially when there is a need for technical developments. This lack of capacity is one of the main reasons why many of the important recommendations from the previous evaluation are not yet implemented. Moreover, this situation endangers the implementation of the new European instruments related to police cooperation and information systems.

Regarding data protection, **overall Estonia complies with the data protection requirements.** Shortcomings are related to e.g. the timely auditing of the national Schengen and Visa Information Systems data processing operations by the Estonian Data Protection Inspectorate, the lack of personnel profiles for access to the Schengen Information System data, the need to improve a number of data security aspects in the use of the National Schengen and Visa Information Systems, that the roles and responsibilities of the data controller and processor for the National Visa Information System are unclear and that there is no monitoring of the Ministry of Foreign Affairs of the data processing by embassies/consulates in the National Visa Information System. Furthermore, data subjects can exercise their right of access in the context of Schengen and Visa Information Systems only in person or by state accredited e-signature from Estonia or from another EU Member State.

Even though, overall, the Estonian authorities implemented most of the recommendations issued in the 2018 Schengen evaluation, due to limited resources and lack a of national prioritization, several important recommendations from the previous evaluation are not yet implemented and there are still several recommendations partly implemented or under implementation.

Based on the 2023 Schengen evaluation, the **priority areas for Estonia,** are:

- ✓ Ensure a **more effective use of the Schengen Information System and** a coherent and aligned approach to **border checks** to ensure uniform implementation of procedures, including the efficient use of the relevant databases.
- ✓ Ensure that **elements concerning fundamental rights**, including proactive assessment of risks of refoulement, effective access to legal remedies, including systematic information on and effective access to free legal aid are safeguarded during the return procedure, in particular during accelerated return procedures carried out within 48 hours of apprehension.
- ✓ **Ensure the efficient exchange of information for law enforcement cooperation, especially related to functioning of SPOC,** including the need for a single fully integrated **case management system and adequate training of officials.**
- ✓ **Enhance the operational cross border cooperation** with the neighbouring Member States to meet the current operational and legal requirements by revising current bilateral agreements.

2. RECOMMENDATIONS

The 2023 periodic evaluation of Estonia resulted in 102 recommendations for remedial action aimed at addressing the deficiencies and areas for improvement identified in the evaluation report.

Considering their importance for the overall functioning of the Schengen area, the implementation of recommendations number 16, 17, 18, 19, 21, 22, 23, 28, 47, 52, 54, 66, 67, 69, 89, 92, 97, 98, and 100, highlighted in bold, should be prioritised.

Recommendations number 19, 22, 23, 40, 67, 92, 96, 97, 98, 100 and 102 relate to persistent deficiencies which have already been identified in the previous Schengen evaluation of Estonia.

Estonia is recommended to:

NATIONAL SCHENGEN GOVERNANCE

National strategies and quality control mechanisms

1. ensure that national strategies include clear strategic goals and prioritisation related to the implementation of the Schengen acquis, in particular development of the cross-border law enforcement cooperation and exchange of information between law enforcement authorities based on the latest EU legal instruments. National Strategies should adequately address recommendations made by the Schengen evaluation related to the implementation of the Schengen acquis;

2. ensure that the national quality control mechanism covers the sea border surveillance, in particular the Navy;

National capabilities

3. ensure the availability of sufficient numbers of staff for return as well as for border checks and border surveillance, in particular in the East Prefecture, the National Coordination Centre and the Regional Coordination Centre in Tartu, in accordance with the operational needs and the results of risk analysis;

4. develop a human resources strategy to address the increasing challenges in internal security and transnational serious and organised crime. Ensure relevant resources for the effective implementation of the Schengen acquis in the area of police cooperation, taking fully into account the new developments in this area;

5. strengthen the capacity of the responsible entity within the Police and Border Guard Board to monitor, identify and absorb EU funds for internal security. Priority should be given to the implementation of the recommendations of the Schengen evaluations;

6. ensure that specialized and refresher trainings on border check related matters are regularly and systematically delivered to the border guards, and that their attendance is mandatory;

7. provide regular training on SIS and SIRENE related matters to the end users in Estonia;

8. ensure that end users of PIKO and APOLLO are more comprehensively trained in using the query tools of PIKO and APOLLO in connection to the functionalities in SIS in order to increase the general knowledge among border guards in the east and south prefectures. Provide periodic and continuous training for end users in order to keep up a good and sound knowledge of the systems

and the SIS. The Estonian authorities are also encouraged to provide on-line training material on SIS that can be easily found and used by the end users;

9. Ensure that the police training curricula cover all relevant instruments of international law enforcement cooperation and guarantee the allocation of sufficient training hours for their completion, as well as ensure proper awareness of the possibilities and activities provided by CEPOL;
10. ensure that by 12.12.2024, SPOC staff is offered regular training courses, provided both at international and national levels, which correspond to their professional needs and specific backgrounds, taking into consideration the provisions of Directive (EU) 2023/977 on the exchange of information between the law enforcement authorities of Member States;
11. develop an interactive and user-friendly e-learning solution on international police cooperation based on practical situations and cases. This solution should encompass the possibility of performance assessment;
12. deliver methodologically robust, well-structured and practice-oriented, sufficiently detailed training – in increased hours – for border guards on fundamental rights in the context of border management, including regular and specialised refresher courses;
13. increase the knowledge and capacity within the Police and Border Guard Board to detect (potential) victims of trafficking in human beings and systematically refer them to appropriate procedures;

Functioning of the authorities

14. urgently transpose Directive (EU) 2019/1937 into national law and introduce procedures for the effective implementation of the new framework. Once this Directive has been transposed, the awareness of staff of the Police and Border Guard Board and other law enforcement agencies of the reporting procedures in place and the protection afforded to whistle-blowers should also be raised;
15. Introduce a legal framework to allow for in-service monitoring of police officers posted to high-risk positions;

Fundamental rights

16. **ensure that the principle of non-refoulement is systematically respected in accordance with Article 5 of the Return Directive, by establishing procedures that allow for a proactive and individualised assessment prior to issuing a return decision, including cases of issuing a return decision within 48 hours after apprehension** *(prioritised recommendation);*
17. provide regular training on the assessment of risks of refoulement to officials in charge of returns of illegally staying third country nationals;

Large scale IT systems (focus on SIS) and data protection

18. **ensure the implementation of all the dactyloscopy searches Fast Print Search, Common Print Search, Mark to Print, Mark to Mark against SIS AFIS in all the relevant applications, in accordance with Article 9(1) and Article 33(2) of Regulation (EU) 2018/1861, Article 9(1) and Article 43(2) of Regulation (EU) 2018/1862 and Article 19 of Regulation (EU) 2018/1860, as applicable to return alerts** *(prioritised recommendation);*

19. **ensure that all search functionalities of the SIS are implemented pursuant to Article 9(2) of Regulation (EU) 2018/1861 and of Regulation (EU) 2018/1862.** *(prioritised recommendation)*[1]*;*

20. improve the security of the secondary data centre by restricting the access to the area and installing a security gate and ensure the business continuity by providing the data centre with a dedicated UPS, *in compliance with Article 10(1) of Regulation (EU) 2018/1861 and of Regulation (EU) 2018/1862*;

21. **provide the necessary additional human resources to the SIRENE Bureau Estonia and enhance automation to ensure the timely and effective exchange of supplementary information** *(prioritised recommendation)*;

22. **introduce an automated, structured, and standardised hit reporting form for the reporting of hits by the end users to the SIRENE Bureau** *(prioritised recommendation)*[2]*;*

23. **ensure the automatic and timely insertion of alerts on missing persons (including minors) and vulnerable persons at risk of being abducted into SIS when creating those alerts in the national database**[3] *(prioritised recommendation);*

24. ensure the technical possibility to create all types of object alerts and unknown wanted person alerts for the purposes of identification as provided for in Article 38(2) and Article 40 of Regulation (EU) 2018/1862;

25. ensure that the retention period for logs is amended as provided for in Article 12(4) of Regulation (EU) 2018/1861 and of Regulation (EU) 2018/1862;

26. provide access to SIS to Customs officers to ensure that all the persons, vehicles and objects that are subject to customs checks are also checked against the SIS and establish, if and where relevant, an agreement between the Estonian Tax and Customs Board and police authorities about hit handling procedures in accordance with their respective national competences, pursuant to Article 34 (1)(b) of Regulation (EU) 2018/1861 and Article 44 (1)(b) of Regulation (EU) 2018/1862;

27. ensure that officers are provided with a transliteration tool to query characters not present in the Estonian alphabet and to correctly enter data when issuing alerts with special characters;

28. **ensure that the list of results in the national applications used to query the SIS is adapted in such a way that the obtained search results are easy to process, such as grouping all identities of a same alert in one alert (containing several aliases), sort the alerts by relevance and/or by order of priority, and display the type of alert**. *(prioritised recommendation);*

29. establish a procedure to delete downloaded data and further enhance the iSPOC application to display photos;

30. ensure that the warning markers are highlighted as a result of a query of a SIS alert in Information System POLIS-KAIRI and that the photos of the perpetrator and the victim of misused identity are displayed in a clear way for the end user to identify the subject of the alert;

[1] Former recommendation 3 of Council Implementing Decision 14872/19 of 05.12.2019
[2] Former recommendation 15 of Council Implementing Decision 14872/19 of 05.12.2019
[3] Former recommendation 13 of Council Implementing Decision 14872/19 of 05.12.2019

31. urgently improve the national APOLLO search application on desktop and all mobile devices in order to carry out single searches for objects and individuals so as to have the results from various national and international databases (SIS and relevant Interpol databases), whilst also ensuring that instructions on the actions to be taken are clear to the end-users by delivering regular refresher trainings;

32. further develop the APOLLO application to display the object extension allowing the end users to identify the data subject in accordance with Article 9(3) of Regulation (EU) 2018/1862;

33. ensure that the misused identity extension, all available photos and the identity document description in the APOLLO application for mobile phone are displayed to allow identification of the subject of the alert in accordance with Article 9(3) of Regulation (EU) 2018/1862;

34. ensure that the applications for querying SIS are capable of searching for all types of objects as provided in article 38 of Regulation (EU) 2018/1862;

35. further develop Information System POLIS to ensure that the search results display the full data of the alert;

36. ensure that all available photos are displayed in PIKO, enabling the officer to clearly distinguish between the photo of the victim and the photo of the perpetrator and to perform their tasks in line with Article 9 (3) of Regulation (EU) 2018/1861 and of Regulation (EU) 2018/1862 and ensure that the applications for querying SIS are capable of searching for all types of objects as provided in article 38 of Regulation (EU) 2018/1862;

37. ensure that in case of a hit in PIKO on discreet, specific and inquiry checks with "Immediate reporting" in the Action to be taken, the text "Contact the national SIRENE Bureau immediately" is displayed in a more prominent way to the end users;

38. implement a standardised hit reporting procedure, supported by a standardised form for hit reporting in order not to miss any relevant and important information;

39. ensure that the reason or purpose for individual consultation of the National Register of the Schengen Information System is required to be provided by the user and recorded in the logs regarding SIS queries;

40. create end-user profiles that describe the functions and responsibilities of authorised persons and define access to Schengen Information System alerts according to individual task-related requirements in line with Articles 10 (1) (h) and 52 of the SIS Regulation 2018/1862 (personnel profiles)[4];

41. ensure that the login process to the applications/databases with access to the Schengen Information System is amended so that the user session and its ending is always tied to the removal of the ID card;

42. amend the criteria for time-out of computer users sessions to require shorter time-out periods for workstations in specific work environments e.g. a busy police station with open office spaces;

43. ensure that passwords for accessing databases which grant access to Schengen Information System data must be changed more frequently than once a year;

44. ensure that internet browsers with a connection to open internet on electronic devices with applications/databases with access to the Schengen Information System should only be allowed when there is a specific work-related need;

[4] Former recommendation 20 of Council Implementing Decision 12870/20 of 12.11.2020

45. ensure that USB ports on computers using applications/databases with access to the Schengen Information System should only be allowed when there is a specific work-related need;

46. adopt the same procedure for entering the server rooms at the different SMIT (Information Technology and Development Centre at the Ministry of the Interior) data centres by always using a RFID card plus a personal PIN code;

47. **ensure that the Police and Border Guard Board finds an alternative for a state accredited electronic e-signature (from Estonia or from another EU Member State) or identification in person at a police station, Estonian Border crossing point or service office as a formal requirement for filing a data subject's rights request in relation to Schengen Information System data processing** *(prioritised recommendation)*;

48. revise the standard replies to distinguish cases where personal data of the data subject are not processed in the Schengen Information System at all and cases in which personal data of the data subjects are processed but there are legal restrictions for the (full) release of those data; information on the reasons of a refusal or restriction of information should be provided unless this would undermine the reasons for the refusal or restriction; also the reply to data subjects requesting correction of personal data must include information on redress;

Data protection supervision

49. ensure that during the budgetary procedure the Parliament is being informed if the overall budget proposal deviates from the budget proposal of the Data Protection Inspectorate;

50. ensure that the recommendation on the requirement of making a data subjects' rights request only in person or via state accredited e-signature from Estonia or from another EU Member State will also be followed up for the Data Protection Inspectorate;

51. ensure independent data protection supervision of the processing of personal data in the National Register of the Schengen Information System and in the Visa Register carried out by the Internal Security Service and the Estonian Foreign Intelligence Service in as far as the Data Protection Inspectorate is not competent to supervise this;

52. ensure that the Data Protection Inspectorate carries out an audit of data processing operations in the National Register of the Schengen Information System at least every four years in accordance with Article 69(2) of Regulation 2018/1862, Article 55 (2) of Regulation 2018/1861 and Article 19 of Regulation 2018/1860 *(prioritised recommendation)*;

53. ensure that the Data Protection Inspectorate carries out frequent inspections of end-user authorities with access to Schengen Information System data, and carries out checks of the National Register of Schengen Information System logs;

54. ensure that the Data Protection Inspectorate carries out an audit of the data processing operations by the responsible visa/Visa Information System authorities, including carrying out on-site inspections of the Ministry of Foreign Affairs, at least every four years in accordance with Article 41(3) of VIS Regulation and Article 8 (6) of VIS Council Decision *(prioritised recommendation);*

55. ensure that the Data Protection Inspectorate carries out regular inspections of a broader variety of end-user authorities with access to the Visa Information System, and carries out regular checks of Visa Register logs;

EXTERNAL DIMENSION

Visa and data protection

56. reinforce and formalise the monitoring of the external service provider by carrying out regularly announced and unannounced visits by the consul; draft reports of the visits and ensure the follow-up of the problems identified;

57. instruct the consulate to systematically carry out checks on the admissibility requirements during the registration phase of the applications;

58. ensure that for repeat applicants who did not provide fingerprints at the external service provider, the consulate systematically verifies whether fingerprints are already stored in the Visa Information System as part of an earlier application and copies them into the new application; refrain from returning such applications to the external service provider without checking the Visa Information System first;

59. refrain from returning admissible applications to the external service provider because some supporting documents are missing; ensure that these applications are accepted and entered in the Visa Information System following their receipt from the external service provider;

60. reconsider the division of responsibilities and tasks of the locally employed staff, the consul and the central authorities , taking into account that the consul is the best placed to assess the local circumstances and migratory risk;

61. ensure adequate supervision of the local staff;

62. ensure that the motivation of the refusal is systematically recorded in the national IT-system;

63. conduct interviews at least on a random basis with first-time applicants and in cases when conflicting information is obtained from the supporting documents;

64. ensure that the 'cascade' mechanism of issuing multiple-entry visas with long validity is consistently and systematically applied;

65. establish the legal basis of the judicial appeal against refusals and provide written information about it;

66. clarify the roles of controller and processor with regard to the processing of personal data in the Visa Register in line with EU law; *(prioritised recommendation);*

67. ensure that the Ministry of Foreign Affairs regularly monitors the processing of Visa Information System data in the Visa Register/, including the establishment of procedures for and analysis of log files in order to check the lawfulness of the data processing; *(prioritised recommendation)*[5]*;*

68. establish a specific procedure to detect and notify data breaches regarding Visa Information System data within the Ministry of Foreign Affairs, including embassies and consulates as well as External Service Providers;

69. ensure that sufficient monitoring and deletion procedures are established with regard to personal data processed in KOMET, including Visa Information System and logging data; *(prioritised recommendation);*

70. ensure that the Data Protection Officer of the Ministry of Foreign Affairs has sufficient capacity

[5] Former recommendations 13 and 14 of Council Implementing Decision 12870/20 of 12.11.2020

to be more actively involved in Visa Information System related data protection matters and his or her independency is not compromised by other tasks;

71. ensure that those recommendations on data protection aspects concerning the management of the National register of the Schengen Information System (40-48) are also followed up for the management of the Visa Register by the Police and Border Guard Board;

MANAGEMENT OF THE EXTERNAL BORDERS

National and European situational awareness and early warning system

72. establish the operational layer of the National Coordination Centre in accordance with Article 24(1) point (b) of Regulation (EC) 2019/1896 on the European Border and Coast Guard by integrating the operational pictures at the land and sea borders;

73. develop the analysis layer of the national situational picture in accordance with Article 24(1) point (c) of Regulation (EC) 2019/1896 on the European Border and Coast Guard. by uploading relevant risk analysis products;

74. ensure that the National Coordination Centre establishes a comprehensive national situational picture by combining information from all borders at operational level;

75. ensure the usage of services provided by Frontex (such as Frontex Vessel of Interest Database, the Fusion Services, and others) and that necessary specialized and refresher trainings are provided for the staff of the Maritime Operational Centre;

76. ensure that complete situational picture at the sea border created by the Maritime Operational Centre is available to the National Coordination Centre in near-to-real time (including effective information exchange, patrol boat positions as well as the maritime traffic situation in the surveillance area) in accordance with Article 21(3) point (d) of Regulation (EU) 2019/1896;

77. ensure that the National Coordination Centre performs the necessary tasks, in particular related to the establishment of comprehensive national situational picture, national picture on resources for border control and has the capacity to support the coordination of border control, as requested by Article 21(3) point (c), (d), (e) and (f) of Regulation (EU) 2019/1896;

Risk Analysis

78. ensure the preparation and use of specific risk profiles at Tallinn airport and Luhamaa Border Crossing Point and assure awareness of risk analyses products by border guards during border check;

Border Surveillance

79. finalize and further develop the integrated land border surveillance system, in particular the stationary surveillance along the entire border with the Russian Federation; ensure and guarantee sufficient financing of this system by also making use of EU funding;

80. improve the capacity to detect and intercept unauthorized cross-border unmanned aerial vehicles (UAV) flights;

Border Checks

81. bring the procedure of border checks in accordance with Article 8 of the Schengen Borders Code by allowing vehicles to be directed immediately to the border crossing point without having to make use of the waiting area;

82. ensure that the mobile devices (Chameleon) can read the chip data for verification and identification of all documents with electronic medium storage (chip); as required by Article 8(2) last paragraph of the Schengen Borders Code;

83. ensure that the procedure of visa verification is in compliance with Article 8(3)(b) of the Schengen Borders Code and Article 18 of Regulation (EC)2008/767 so that proper verification of the authenticity of the visa can be carried out;

84. ensure the protection of personal data in the visa issuing procedure by establishing a procedure to delete photos of visa applicants to be attached to the "Application for Schengen Visa" from work mobile phones and workstations of Border Guard officers as soon as possible;

85. bring the procedure of issuing visas at the border in accordance with Article 35 of Regulation (EC) No 810/2009 of the European Parliament and of the Council;

86. ensure proper supervision of the ABC gates, for example by using the dedicated booth behind the ABC gates, facing the passenger flow;

87. adopt a procedure for discreetly collecting information in case of hits on alerts for discreet checks at the ABC gates as to not jeopardise the discreet nature of the checks and to not make in any way the subject of the alert aware of the existence of the alert in line with Article 37.3 of Regulation (EU) 2018/1862;

88. bring the practice of imposing fines to air carriers in compliance with Article 26(2) of the Schengen Convention and Article 4 of Council Directive 2001/51/EC of 28 June 2001;

NATIONAL RETURN SYSTEM

89. amend the national legislation within the meaning of Article 3(4) of Directive 2008/115/EC as well as the respective templates, to ensure the obligation to return has an EU/Schengen wide effect. *(prioritised recommendation);*

90. systematically provide third-country nationals subject to return procedures with access to legal advice and free legal assistance in compliance with Article 13 (3) and (4) of Directive 2008/115/EC. Improve information provision about legal aid possibilities, while ensuring efficient modalities to access effective remedy in a timely manner prior to removal in accordance with Article 13 (1) of the same Directive;

91. ensure the effectiveness of the forced return monitoring system in accordance with Article 8 (6) of Directive 2008/115/EC, by ensuring that the forced-return monitoring body is notified about all planned forced returns, and improving the transparency of the monitoring, especially as regards publication of the main recommendations resulting from monitoring activities;

MEASURES WITHIN THE AREA OF FREEDOM, SECURITY AND JUSTICE

Exchange of information for cross-border and international police cooperation

92. further develop the central entity (SPOC) responsible for coordinating and facilitating the exchange of cross-border law enforcement information and ensure that the Single Point of Contact is provided with adequate number of qualified staff, appropriate operational tools, technical and financial resources, infrastructure, and capabilities, necessary to carry out its tasks in an adequate, effective and rapid manner, by 12 December 2024. *(prioritised*

recommendation)[6]*;*

93. ensure that a dedicated unit within the SPOC performs all the tasks listed in Article 7 of the Regulation (EU) 2016/794, such as supplying Europol with the information necessary for it to fulfil its objectives and ensuring effective communication and cooperation of all relevant competent authorities with Europol;

94. establish a clear division of tasks within the SPOC and a clear chain of assignments towards the responsible entities and proper monitoring of information flow via SIENA;

95. develop a technical solution to provide law enforcement officers with computerised access to registers of establishments providing accommodation for short-term stays in accordance with national law, subject to adequate data protection safeguards;

96. develop clear and detailed written guidelines regarding the rules of cross-border information exchange, choice of international law enforcement cooperation tools and communication channels (listing for instance practical examples)[7];

97. develop a Case management system for the Single Point of Contact with the automation of information processing, the function to record, in an automated manner, any relevant communication or exchange of information between the SPOC and the national competent authorities or between the SPOC and the competent authorities of other Member States, including the integration of Europol's Secure Information Exchange Network Application (SIENA) by 12 December 2024. *(prioritised recommendation)*[8];

Operational cross border police cooperation

98. **revise bilateral and/or multilateral cross-border cooperation agreements to include provisions on operational law enforcement cooperation in line with Council Recommendation (EU) 2022/915 on operational law enforcement cooperation, as well as develop a formal review mechanism for bilateral and/or multilateral cooperation agreements with the aim to increase their operational effectiveness.** *(prioritised recommendation)*[9]*;*

99. enhance the quality and capacity of the communication in cross-border cooperation by preparing the technology, application eco-system and procedures for the use of the EU Critical Communication System within the BroadEU.net;

100. **ensure full implementation and awareness of the access procedure for law enforcement purposes to the Visa Information System established under the Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection, and investigation of terrorist offences and of other serious criminal offences.** *(prioritised recommendation)*[10]**;**

Cooperation with Europol

101. improve information exchange with Europol by establishing clear procedures on sharing information with Europol, respecting all conditions laid down in Regulation (EU) 2016/794 and

[6] Former recommendations 1 and 2 of Council Implementing Decision 11061/19 of 8.07.2019
[7] Former recommendations 10 of Council Implementing Decision 11061/19 of 8.07.2019
[8] Former recommendations 1, 2, 3 and 8 of Council Implementing Decision 11061/19 of 8.07.2019
[9] Former recommendation 4 of Council Implementing Decision 11061/19 of 8.07.2019
[10] Former recommendation 11 of Council Implementing Decision 11061/19 of 8.07.2019

the Council Framework Decision 2006/960 (as well as Directive (EU) 2023/977 when in force from 12 December 2024);

102. introduce an automated data loader to the Europol Information System and ensure that criminal information obtained within ongoing investigations is uploaded when it relates to serious and organised crime and terrorism[11].

11 Former recommendation 13 of Council Implementing Decision 11061/19 of 8.07.2019