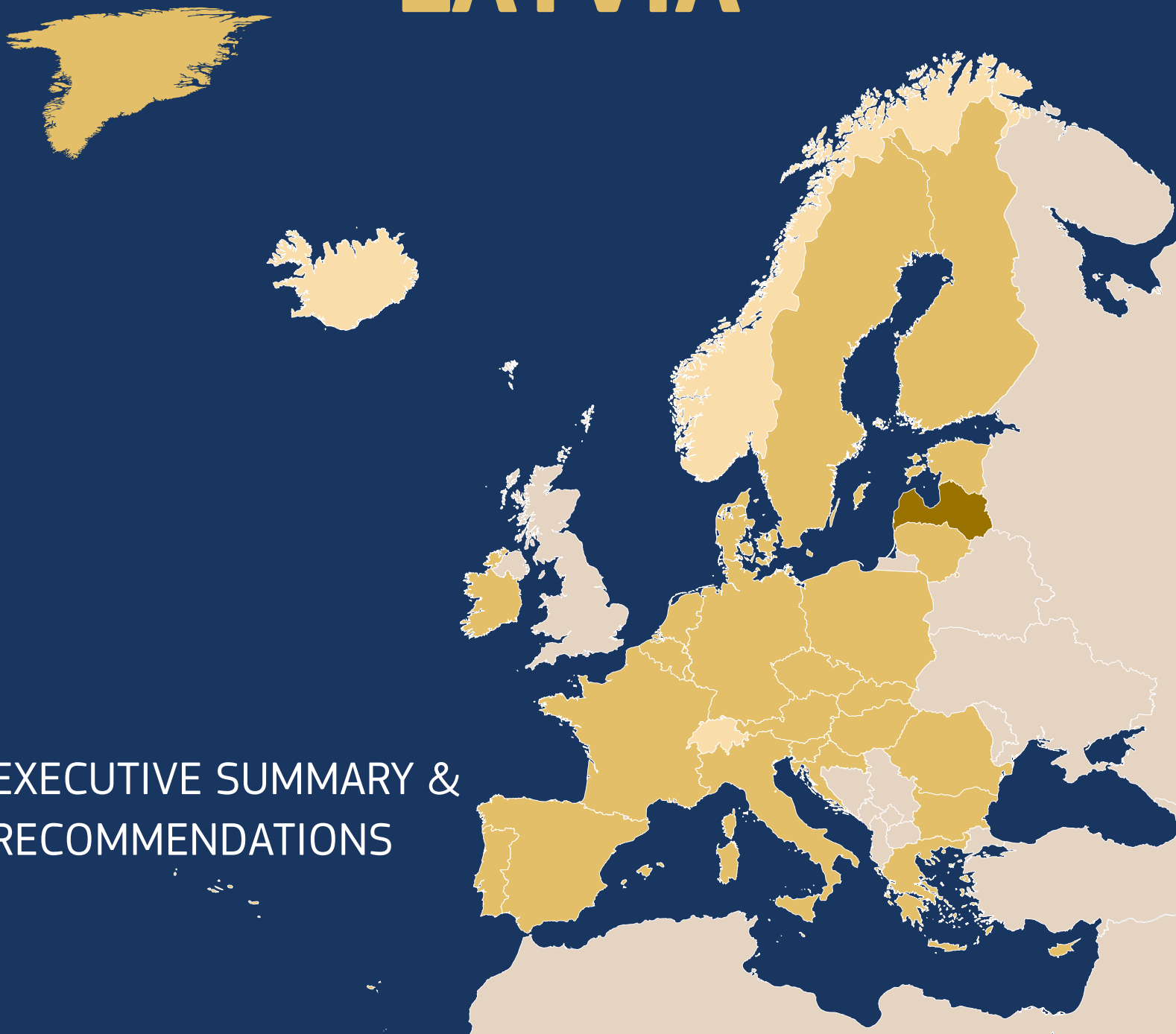
European Commission

Schengen Evaluation of **LATVIA**



EXECUTIVE SUMMARY & RECOMMENDATIONS

SCHENGEN EVALUATION OF LATVIA 2023

EXECUTIVE SUMMARY AND RECOMMENDATIONS

1. EXECUTIVE SUMMARY

A Schengen evaluation of Latvia was carried out in the period October - November 2023 by Commission and Member State experts accompanied by observers from relevant 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 also paid to verifying the respect for fundamental rights. This activity results in the report of the 2023 Schengen evaluation of Latvia.

Latvia has been facing serious challenges at its external borders caused by the **instrumentalisation of migration** by Belarus since 2021, and by Russia's military invasion of Ukraine since 2022. This has led to a significant increase in the number of third country nationals irregularly crossing the green border (from 53 in 2019 to 455 in 2021 and 277 in 2022)[1], and high numbers of arrivals to border crossing points of Ukrainian refugees, which severely affected the external border management and migration structures, particularly for return. The pressure has led Latvia to amend its national law and introduce measures declaring an enhanced border protection regime, with focus on the regions bordering Belarus. These legal changes have an **important impact on the protection of fundamental rights of third country nationals**, specifically on *non-refoulement* safeguards.

Latvia also commenced the construction of a physical barrier at its external borders and requested support for border control from the Latvian Armed Forces and Frontex. While the **performance of border control** is currently at an adequate level to handle the crisis situation, the mentioned support is especially important due to Latvia's difficulties to fill the available vacancies in respective services, causing a long-standing shortage of staff not only for border control and return, but also for police and data protection tasks.

Notwithstanding the migration challenges faced, **the overall implementation of the Schengen *acquis* by Latvia is adequate** with the exception of the implementation of **large-scale information systems**, given that the Schengen Information System (SIS) and SIRENE procedures are not well integrated in the border, migration and law enforcement processes. At the same time, it was noted that a number of recommendations issued following the 2018 Schengen evaluation of Latvia remain unaddressed in all policy areas, with the highest concern for the Schengen Information System, leading to persistent deficiencies and repeated recommendations, as underlined further in the report.

The **implementation of the European integrated border management in Latvia was assessed as adequate**. The State Border Guard Service being the main responsible service for border control, prevention of illegal migration and return in Latvia, operates based on a well-

[1] Data provided by the Latvian authorities.

developed risk analysis system. It is also the main coordinating body for border security. The basic training system for border guards is robust, providing well prepared staff for border control and contributing to a good quality of border control. However, the challenge of limited staff numbers was noted affecting the quality of border control and return.

For the purposes of external border management and return, Latvia ensures a **good level of interagency cooperation** based on national legislation and written interinstitutional agreements. The national and regional contingency plans for emergency situations and a national capability plan are available and tested in real operational situations. At national level, the plans also foresee the role and tasks of the Border and Coast Guard Agency (Frontex) Standing Corps and the European Union Agency for Asylum, although such involvement is not mentioned in regional contingency plans. Latvia has a well-developed national quality control mechanism, revised in 2020 to cover the applicable Schengen *acquis* for border checks and border surveillance. .

The land and maritime surveillance systems ensure **an adequate level of border surveillance**. However, **Eurosur is not implemented** as only the event layer is regularly used, while analysis and operational layers are not complete, negatively affecting the completeness of the national situational picture.

Challenges in the area of return are closely connected to the persistent deficiencies remaining from the previous Schengen evaluation as well as new findings relating to non-issuance of return decisions in certain cases, procedural guarantees and the use of alternatives to detention.

The most important finding, observed both from the perspective of return and external border management, is linked to the amendments in the national law and the measures related to an enhanced border protection regime, which has an **impact on the level of protection of fundamental rights.** All third-country nationals who cross the land border with Belarus in an unauthorised way are redirected to the Belarusian side of the border. Persons requesting asylum are admitted only if this is justified on humanitarian grounds based on a limited on-the-spot assessment, *i.e.,* if they have visible signs of vulnerability. According to the Asylum Law, international protection applications can be submitted only at border crossing points facilities and thus, there is no possibility in this regard for migrants apprehended at the green border.

Finally, a good practice was reported as regards mutual recognition of return decisions, which is used on a regular basis, thus speeding up the return process.

Latvia has a **contingency plan** for the mass influx of asylum seekers and the National Capability Development Plan in the field of border management and return, which sets a list of national priorities and actions for these two areas.

As far as the implementation of the **EU visa *acquis*** is concerned, **Latvia complies** with the Visa Code and other relevant legislation. The examination of the applications is solid and decisions are well-founded. The staff has a good knowledge of the EU law and is experienced in Schengen visa processing.

In the area of **police cooperation**, Latvia is **in general implementing the Schengen *acquis* adequately.** The internal security system is well established, and interagency law enforcement cooperation is clearly regulated and implemented. The Latvian law enforcement system is

adequately connected to European law enforcement cooperation structures, including to well-established cooperation with Europol and involvement in EMPACT activities. Well established and comprehensive common annual planning system for practical bilateral cross border cooperation with the neighbouring countries of the Schengen area was considered **as a best practice**. Awareness of the Code of Ethics for the State Police (adopted 5 February 2020) and new Whistleblowing Law (2 February 2022) among the police staff was found to be at adequate level.

As regards the **Schengen Information System (SIS)**, Latvia was evaluated on the implementation of the renewed SIS with enhanced functionalities, which entered into operations on 7 March 2023. The evaluation team concluded that the **Schengen *acquis* in the field of large-scale information systems is not well implemented**. Further improvements should be made to ensure a more effective use of the SIS. Considering the number and type of findings, in particular related to the implementation of all the functionalities of the renewed SIS, the network stability, full access to SIS to Migration authorities as well as the use of alerts on return and the full roll out of SIS Automated Fingerprint Identification System (AFIS) to all police authorities, **the team considers it necessary to organise a verification visit**, to check the progress on the implementation of the renewed SIS.

In the policy area of **data protection**, Latvia was assessed to have an **overall adequate level of compliance with the Schengen *acquis***. Nevertheless, there are still deficiencies including the fact that the Data State Inspectorate does not have complete independence as required by the Schengen *acquis*. Other findings included the need to eliminate the conflict of interest stemming from other tasks of the persons assigned the role of the data protection officers in the Latvian State Police and the Office of Citizenship and Migration Affairs, requirement to have security plans for Visa Information System (VIS) and Schengen Information System (SIS) as well as ensure biometric data quality in line with the threshold of eu-LISA.

On the basis of the 2023 Schengen evaluation, the following priorities were established in this report. They are to be addressed by Latvia by implementing recommendations issued for the corresponding policy area:

1. *Ensure the* ***respect of fundamental rights****, especially in relation to the principle of non-refoulement, in connection to border control measures.*

2. *Ensure* ***full implementation of the renewed Schengen Information System (SIS)****.*

3. *Address the* ***long-standing shortage of staff*** *to implement border control, return, data protection and police tasks.*

4. *Ensure* ***complete independence of the Data State Inspectorate*** *by amending the national legislation, by aligning the law governing the Data State Inspectorate with the law governing the Latvian Ombudsman.*

2. RECOMMENDATIONS

The 2023 periodic evaluation of Latvia resulted in 90 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 the recommendations number 3, 10, 15, 21, 23, 24, 28, 41, 49, 78, 79, and 86 should be prioritised.

Recommendations 4, 13, 14, 15, 19, 21, 28, 29, 30, 35, 37, 39, 41, 61 and 71 relate to persistent deficiencies which have already been identified in the previous Schengen evaluation of Latvia.

Latvia is recommended to:

NATIONAL SCHENGEN GOVERNANCE

National strategies

1. prepare a national strategy focussing on internal security including clear objectives for international law enforcement cooperation.

National capabilities

2. develop and implement a comprehensive human resources strategy for Latvian State Police;

3. **develop an effective short-term strategy to ensure adequate staffing levels in the State Border Guard Service for effective and efficient border control and to conduct effective returns, e.g. by enhancing the competitiveness and attractiveness of career in the service;** [prioritised recommendation]

4. ensure that the Data State Inspectorate is staffed with a sufficient number of IT experts to carry out the tasks entrusted to it under the Schengen Information System (SIS) and Visa Information System (VIS) acquis, notably by adjusting the Data State Inspectorate's staff remuneration at a level comparable to similar independent bodies, including by increasing the Data State Inspectorate's Director's remuneration[2];

5. provide English language training to all border guards to ensure a sufficient level of communication for carrying out border control tasks, in particular first-line border checks;

6. provide regular refresher trainings on the practical application of fundamental rights and ensure that border guards have an adequate knowledge on how to detect, identify and deal with situations involving vulnerable persons, such as unaccompanied minors and (potential) victims of trafficking in human beings, and systematically refer them to appropriate procedures;

[2] Former recommendation 2 of Council Implementing Decision 12469/19 of 24 September 2019, setting out a recommendation on addressing the deficiencies identified in the 2018 evaluation of Latvia on the application of the Schengen *acquis* in the field of data protection.

7. develop dedicated continuous training regarding the rules of cross-border law enforcement cooperation and information exchange for the staff of the Single Point of Contact (SPOC);

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

9. ensure proper training and common awareness to all end-users of the Schengen Information System on the available tools, the new procedures of the renewed SIS and access rights, data protection and security; Ensure that its effectiveness is evaluated systematically, e.g., through the use of exams, and that the training is mandatory for end-users.

Fundamental rights aspects, including safeguards

10. **in accordance with Articles 19 and 47 of the Charter of Fundamental Rights, Articles 3(b), 4, 7(1) and 13 of the Schengen Borders Code and Article 4(4) of Directive 2008/115/EC: take measures to ensure the full respect of the principle of non-refoulement by establishing procedures that allow for an individualized assessment in each specific case and referral to appropriate procedures, including the access to effective remedy; establish a sufficient assessment procedure that allows detecting vulnerable persons including potential victims of trafficking in human beings, and systematically refer them to appropriate procedures; ensure that third country nationals seeking international protection on the territory, including at the border, can effectively access international protection.** [prioritised recommendation]

Large-scale information systems and data protection

11. ensure that all of functionalities of the SIS are implemented as provided for in Article 9(2) of Regulation (EU) 2018/1862;

12. ensure that the SIRENE Bureau always attach EAW when creating alerts on wanted persons in line with Article 27(1) of Regulation (EU) 2018/1862;

13. ensure that missing persons are always inserted in the SIS[3];

14. ensure the full use of the linking functionality in SIS[4];

15. **establish a clear procedure and a technical solution to always attach fingerprints to alerts when they are available[5];** [prioritised recommendation]

---

[3] Former recommendation 12 of Council Implementing Decision 5798/19 of 28 January 2019, setting out a recommendation on addressing the deficiencies identified in the 2018 evaluation of Latvia on the application of the Schengen *acquis* in the field of the Schengen Information System.

[4] Former recommendation 20 of Council Implementing Decision 5798/19 of 28 January 2019.

[5] Former recommendation 1 of Council Implementing Decision 5798/19 of 28 January 2019.

16. ensure that deletion and archiving procedures of personal data in SIS are carried out in line with Article 57 of Regulation (EU) 2018/1862;

17. ensure that all supplementary information exchanges on alerts in the SIS is available in the SIRENE Case Management System, in line with Article 9(3) Regulation (EU) 2018/1861 and Article 9(3) Regulation (EU) 2018/1862 and, as applicable to return alerts, Article 19 of Regulation (EU) 2018/1860;

18. implement a technical solution to perform automatic checks in SIS to validate alerts to ensure the compatibility and the priority of alerts as foreseen in Article 23 of Regulation (EU) 2018/1862, Article 23 of Regulation (EU) 2018/1861, and as applicable to return alerts, Article 19 Regulation (EU) 2018/1860;

19. ensure that the SIRENE Bureau is provided with the necessary human and technical resources, including further automatization, to perform the tasks assigned, e.g. by creating the possibility in the end-user applications to send a hit report to the SIRENE Bureau in an automated and secure way[6];

20. ensure that the tool for automated collection of statistical data integrated in the SIRENE Case Management System is able to produce reliable statistical data;

21. **ensure full and direct access to the Schengen Information System for the Office of Citizenship and Migration Affairs and the Customs[7], in line with Articles 34 of Regulation (EU) 2018/1861, Article 44 of Regulation (EU) 2018/1862, and, as applicable to alerts on return, Article 19 of Regulation (EU) 2018/1860, and establish the follow-up procedures for the OCMA in case of a hit, in line with Article 44 of Regulation (EU) 2018/1862;** [prioritised recommendation]

22. ensure that SIS is integrated in the national systems via a single interface to guarantee that SIS is systematically checked when performing a search in line with Article 1 of Regulation (EU) 2018/1861 and Article 1 of Regulation (EU) 2018/1862;

23. **implement the fingerprint searches for SIS AFIS for State Police and the Office of Citizenship and Migration Affairs (OCMA) in line with Article 9(1) and Article 33(2) of Regulation (EU) 2018/1861 and Article 9(1) and Article 43(2) of Regulation (EU) 2018/1862, and Article 19 Regulation (EU) 2018/1860, as applicable to return alerts;** [prioritised recommendation]

24. **ensure that the e-LIETA application consistently displays the results of queries as foreseen in Article 9(2) Regulation (EU) 2018/1861 and Article 9(2) Regulation (EU) 2018/1862 and, as applicable to return alerts, Article 19 of Regulation (EU) 2018/1860;** [prioritised recommendation]

---

6 Former recommendation 13 and 17 of Council Implementing Decision 5798 of 28 January 2019.

7 Former recommendation 21 (Customs) of Council Implementing Decision 5798/19 of 28 January 2019.

25. implement the necessary technical changes in the e-LIETA application to ensure the display of all data of the SIS alerts, as required by Article 9(2) and Article 9(3) of Regulation (EU) 2018/1861, Article 9(2) and Article 9(3) of Regulation (EU) 2018/1862, and Article 19 of Regulation (EU) 2018/1860, as applicable to alerts on return;

26. implement the necessary technical changes in the e-LIETA application to ensure that SIS is systematically consulted;

27. ensure that data available in the SIS alert is displayed in a way to enable the end-users to perform the correct follow-up of the alerts;

28. **update the MOBAPP application or cease the use of this application providing different modalities of checks until the new mobile equipment is released, to ensure the application of Article 9(2), Article 9(3) Regulation (EU) 2018/1861 and Article 9(2) and Article 9(3) Regulation (EU) 2018/1862 and, as applicable to alerts on return, Article 19 of Regulation (EU) 2018/1860**[8]; [priority recommendation]

29. ensure that back-ups of N.SIS data are stored in a different physical location to guarantee the security and retrieval of the data in case of an incident, to comply with Article 10(1)(m) of Regulation (EU) 2018/1861 and Article 10(1)(m) of Regulation (EU) 2018/1862 and, as applicable to return alerts, Article 19 of Regulation (EU) 2018/186[9];

30. ensure the appropriate measures are taken in order to guarantee the physical security of the main and back-up data centres[10];

31. implement a national procedure to ensure a high degree of data quality;

32. ensure that information about data subjects' rights in relation to the VIS and the SIS and the standard forms are easy to find on all the relevant websites of the authorities involved in those processing, including with regard to the right to lodge a complaint and judicial remedies in different languages. Ensure that the information provided to the data subject is updated taking into consideration the renewed SIS;

33. improve the procedure to reply to data subject's access requests for their data in SIS, including general data access requests to the State Police, in particular by ensuring case-by-case assessment of each reply;

34. ensure that an appropriate Security Plan (SP), Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) are in place for N.SIS in accordance with Article 10(1) of Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862;

---

8 Former recommendation 10 of Council Implementing Decision 5798/19 of 28 January 2019.

9 Former recommendation 34 of Council Implementing Decision 5798/19 of 28 January 2019.

10 Former recommendation 36 of Council Implementing Decision 5798/19 of 28 January 2019.

35. ensure that authorities with access to N.SIS review log files regularly and systematically, including proactively, in order to determine the lawfulness of data processing[11];

36. ensure that systematic checks of user rights of SIS are conducted on a regular basis;

37. implement two-factor authentication to access N.SIS and N.VIS[12];

38. implement further measures to make impossible to use USB flash drives;

39. ensure that production data is not used for test purposes in order to comply with Article 51 of Regulation (EU) 2018/1861 and Article 66 of Regulation (EU) 2018/1862[13];

40. eliminate conflicts of interest by clearly defining the tasks and powers of the State Police Data Protection Officer and to separate those tasks and the tasks of the Deputy Chief of the Internal Control Bureau and include a formal requirement that the Data Protection Officer of the State Police shall possess expert knowledge of data protection legislation and practices as set out in Articles 32 to 34 of the Law Enforcement Directive and Article 37(5) in conjunction with Article 38(6) of the General Data Protection Regulation.

Data protection supervision

41. **ensure complete independence of the Data State Inspectorate by amending the law governing the Data State Inspectorate for example, by aligning it to the law governing the Latvian Ombudsman**[14]**;** [prioritised recommendation]

EXTERNAL DIMENSION

42. strengthen the national coordination concerning the use of liaison officers; conduct a thorough analysis with the other Baltic countries on the establishment of a common use of these countries' respective liaison officers, as is suggested in Council Decision 2003/170/JHA.

Visa

43. ensure that the territorial competence and admissibility requirements are checked systematically, including whether the correct visa fee is charged, as set out in Article 19 of the Visa Code and Article 8 of Regulation (EC) No 767/2008;

44. ensure that the tasks regarding the verification of supporting documents between the local staff and the consul are complementary and not duplicating;

45. ensure that the travel documents are systematically checked during the examination of applications;

---

11 Former recommendation 17 of Council Implementing Decision 12469/19 of 24 September 2019.

12 Former recommendation 19 of Council Implementing Decision 12469/19 of 24 September 2019

13 Former recommendation 20 of Council Implementing Decision 12469/19 of 24 September 2019.

14 Former recommendation 1 of Council Implementing Decision 12469/19 of 24 September 2019.

46. ensure a swift access to information related to the origin of alerts by, for example, modifying the national visa processing IT-system so that it provides information to the consul on which Member State entered the alert in the Schengen Information System, or by ensuring that the central authority systematically provides a reply without undue delay (e.g. within 24 hours);

47. modify the national visa processing IT-system to prohibit the consul from issuing a uniform visa in case of an entry ban alert in the Schengen Information System;

48. ensure that a digital seal (2D barcode) is printed into box 16 of the visa stickers as set out in Commission Implementing Decision C(2020) 2672;

49. **urgently ensure that the quality of the fingerprints obtained by Latvian authorities is accurate in accordance with Article 5(1) of the General Data Protection Regulation and meets the threshold provided by eu-LISA in all cases;** [prioritised recommendation]

50. ensure that there is a functionality for taking decision of admissibility in the N.VIS and it is not possible to send the application to the VIS without having made a decision on whether or not an application should be considered admissible based on Article 19 of the Visa Code; ensure that the application file is created in the central visa information system (C-VIS) without delay after a decision is taken regarding the admissibility, in line with the Article 19(1) and (2) of the Visa Code and Article 8(1) of the VIS Regulation;

51. ensure that a security plan is created covering all authorities of the visa process in order to ensure the operational security of the visa information system (VIS) in line with Article 32 of the VIS Regulation;

52. ensure logging of failed attempts to log into N.VIS and conduct systematic checks of user rights of VIS on a regular basis in order to ensure the operational security of the visa information system;

53. align the contracts with the External Service Providers with the requirements of the General Data Protection Regulation, notably Article 28;

54. establish a written internal procedure on how to deal with the requests for the exercise of data subject's rights in VIS by the Ministry of Foreign Affairs and the Office of Citizenship and Migration Affairs. Make this procedure transparent to the data subjects;

55. ensure the independence of the Data Protection Officer in charge of the National Visa Information System by separating the functions of the Data Protection Officer from the functions of the Information Security Officer as set out in Article 38(6) of the GDPR.

MANAGEMENT OF THE EXTERNAL BORDERS

National and European situational awareness and early warning system

56. review the standard operating procedure to enable increase of staffing in the shifts of the National Coordination Centre in case of need, and taking into account the current situation

at external land border; reallocate the non-essential tasks to administrative units to ensure the resources of the core function of the National Coordination Centre;

57. increase the number of certified Eurosur operators in the National Coordination Centre;

58. increase the utilisation of analysis layer of Eurosur;

59. establish the operational layer in accordance with Articles 24(1)(b), 25(2)(c), 25(2)(e) and 26(2)(a) of Regulation (EU) 2019/1896 on European Border and Coast Guard and Articles 10 and 11 of Commission Implementing Regulation (EU) 2021/581;

60. ensure completeness of the National Situational Picture in the National Coordination Centre by including the sea border situation in the national situational picture as defined in Article 21(3)(d) and 25(2)(a) of Regulation (EU) 2019/1896 on European Border and Coast Guard.

Risk analysis

61. increase the number of trained officers responsible for risk analysis for sea and air border control at regional and local levels; centralise the responsibility for risk analysis for land border control by assigning the person with main responsibility and a back-up, and establish the order of deputising; ensure that the staff allocated for risk analysis tasks has sufficient time to carry out risk analysis in accordance with the Common Integrated Risk Analysis Model (CIRAM)[15];

62. enhance the frequency of updating risk profiles and risk indicators and ensure the comprehensive awareness of these products among all border guards on duty.

Border surveillance

63. ensure that the Armed Forces officers are used for border surveillance tasks only in a supportive role and under constant direct supervision of competent border guards, and that all the Armed Forces officers supporting the border guards receive an appropriate pre-deployment training for border surveillance tasks, including on fundamental rights, in order to comply with Article 16 of the Schengen Borders Code;

64. establish and ensure a complete maritime situational picture, e.g by enhancing the access to the sea and coastal surveillance system functionalities and dissemination of this picture to the decentralized units;

65. improve the camera surveillance system and ensure the connectivity and operating functions of the camera surveillance systems and other surveillance tools in order to improve the situational picture.

[15] Former recommendation 8 and 9 of Council Implementing Decision 7288/19 of 8 March 2019, setting out a Recommendation on addressing the deficiencies identified in the 2018 evaluation of Latvia on the application of the Schengen acquis in the field of management of the external border.

Border checks

66. improve the knowledge on profiling to reduce the processing time at the border checks at Riga Airport;

67. develop a user-friendly border control system with a single interface that automates searches in order to speed up border checks;

68. ensure stable access to the national system for border control (REIS);

69. ensure that all information in the alert is correctly displayed to the end-user in the REIS application in line with Article 9(2) and (3) of Regulation (EU) 2018/1861, Article 9(2) and (3) of Regulation (EU) 2018/1862, and as applicable to alerts on return, Article 19 of Regulation (EU) 2018/1860;

70. bring the checks of seamen going ashore in compliance with Article 20 read in conjunction with Annex VII, paragraph 3 of the Schengen Borders Code by checking whether they are in possession of seamen's book;

71. ensure that the Advance Passenger Information (API) data is systematically checked against the relevant databases in order to increase its added value for cross border crime and irregular migration, as set out in Article 3 of Council Directive 2004/82/EC of 29 April 2004[16];

72. ensure systematic border checks on pleasure boats and small vessels at the external sea borders as required by Articles 8 and 19 in conjunction with Annex VI, point 3.2.4 and point 3.2.5 of the Schengen Borders Code.

NATIONAL RETURN SYSTEM

73. ensure that third-country nationals are issued return decisions when a residence permit is expired or revoked, and in the absence of a right to reside on another legal basis, in accordance with Article 3(4) of Directive 2008/115/EC.

74. amend the national law, strengthen the practice and national procedures to ensure that third-country nationals are not detained or are immediately released from detention when there is no (or no longer a) reasonable prospect of removal, in line with Articles 15(1) and (4) of Directive 2008/115/EC.

75. amend the national legislation and practice to ensure that detention is used as a measure of last resort; ensure that alternatives to detention can be applied not only in cases limited to humanitarian grounds, in accordance with Article 15(1) of Directive 2008/115/EC;

76. ensure access to a wider variety of leisure activities for detained third country nationals and that the activities offered are also appropriate to their age and needs, outdoors as well as indoors; ensure privacy for detained third-country nationals when interacting with the

[16] Former Recommendation 44 of Council Implementing Decision 7288/2019 of 8 March 2019.

outside world; ensure that meaningful contact with the outside world is not hampered by insufficient means and/or use of space.

MEASURES WITHIN THE AREA OF FREEDOM, SECURITY AND JUSTICE

Exchange of information for cross-border and international police cooperation

77. improve the implementation and monitoring of the actions, needed to respond identified risks, and based on risk analysis from the central level to the regional and local level. Take into account also the cross-border dimension when conducting risk analysis based on National Criminal Intelligence Model;

78. **proceed with the full technical and/or organizational integration of all national Law Enforcement Authorities that need to be involved in cross-border information exchange into the Single Point of Contact structure in order to enable the SPOC to be a hub for all incoming and outgoing international information exchange;** [prioritised recommendation]

79. **urgently improve the Case Management System of the SPOC by increasing the automation of information processing, the capability to search for and cross-check available information into relevant national, EU and international databases in an automated and simultaneous manner, 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);** [prioritised recommendation]

80. urgently improve the national search application on both desktop and mobile devices in order to carry out searches for objects and individuals in one single tool, equipped with fuzzy and any-name search functions; checks into the SIS, EIS and INTERPOL databases should be mandatory and the user should be presented with clear actions to be taken;

81. urgently improve security features of MOBAPP for a secure mobile access to relevant national and international databases

82. ensure direct access to SIENA to investigators from the different competent law enforcement authorities at the central and regional level, and provide corresponding training of end-users;

83. implement the technical solution (lightweight data loader) to insert data from national databases in the EIS. Alternatively, make use of the batch upload to share relevant intelligence/information on criminal investigation to EIS while the data loader solution is not ready;

84. expand a full integration and use of EIS in the national information system for all Law Enforcement Agencies;

85. raise 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 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 and to EURODAC for law enforcement purposes established in Regulation 603/2013/EU of 26 June 201;

86. **develop a technical solution in order to provide law enforcement officers with computerised access to hotel registers in accordance with national law, should the need arise, subject to adequate data protection safeguards.** [prioritised recommendation]

Operational cross-border police cooperation

87. revise bilateral and/or multilateral cooperation agreements to include provisions on operational law enforcement cooperation in line with the 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;

88. improve the operational readiness and awareness on hot pursuit with neighbouring countries by organising regularly (at least annually) mock exercises with neighbouring countries;

89. implement, in partnership with the neighbouring countries, a standardized and secure real time communication system compatible with all neighbouring countries. Prepare the technology, application eco-system and procedures for the use of the EU Critical Communication System within the BroadEU.net.

Cooperation with Europol

90. improve the national capacity to combat serious and organised crime, in particular migrant smuggling, by actively engaging the relevant law enforcement authorities in the relevant EMPACT Operational Actions and by enhancing cooperation of the State Border Guard with Latvian Liaison Officers deployed to Europol, including evaluation of possible deployment of the State Border Guard representative to Europol Liaison Bureau.

***