



Brussels, 23.7.2024
C(2024) 1960 final

ANNEX 2

ANNEX

to the

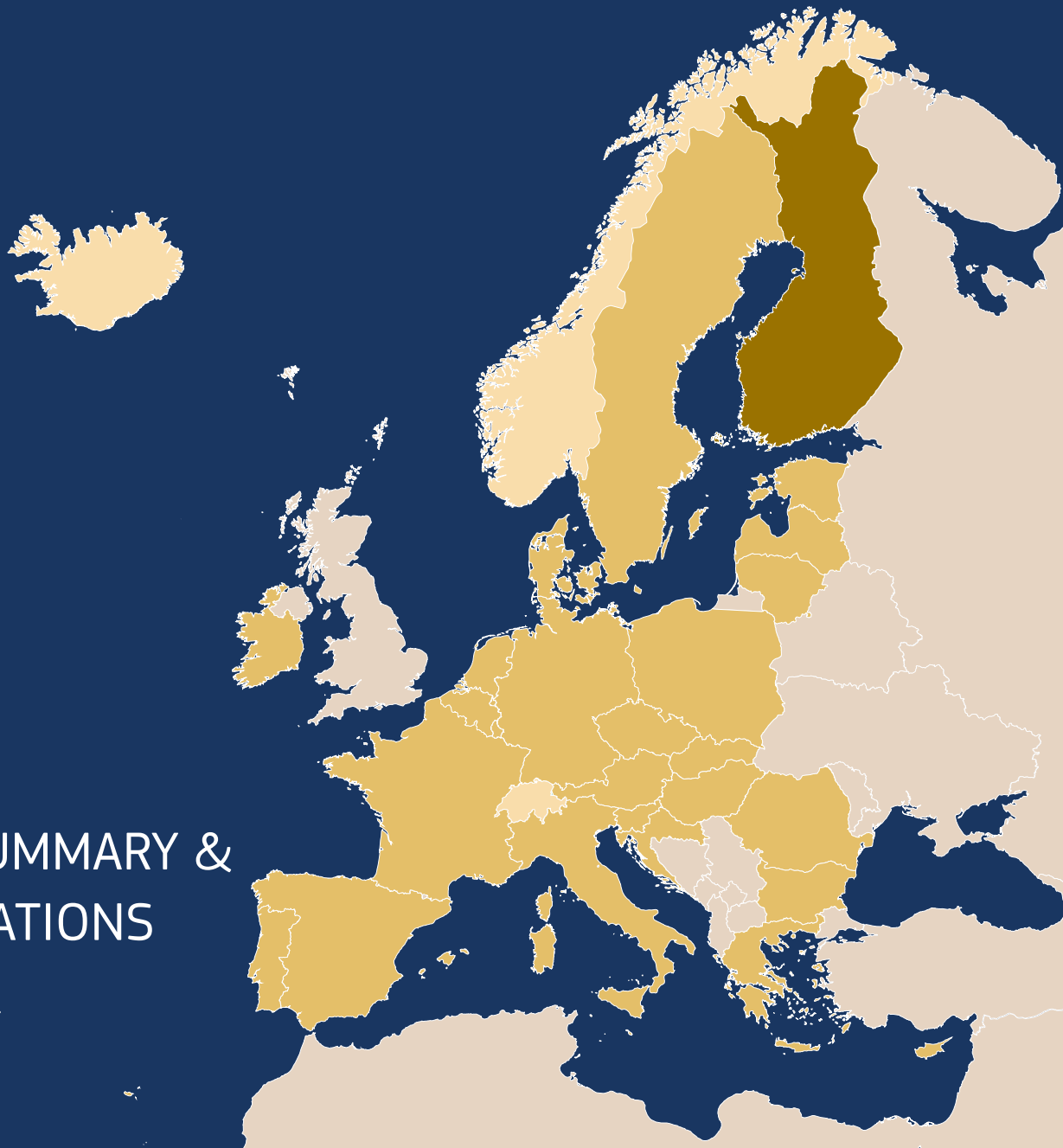
Commission Implementing Decision

establishing the report of the 2023 Schengen evaluation of Finland



Schengen Evaluation of **FINLAND**

EXECUTIVE SUMMARY &
RECOMMENDATIONS



SCHENGEN EVALUATION OF FINLAND
EXECUTIVE SUMMARY OF THE 2023 COUNTRY REPORT
&
RECOMMENDATIONS

1. EXECUTIVE SUMMARY

A Schengen evaluation of Finland was carried out in May and June 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 paid to verifying the respect for fundamental rights. This activity results in the report of the 2023 Schengen evaluation of Finland.

The war of Russia against Ukraine, which started in February 2022, has marked a turbulent period for European security, leading the Finnish Government to seek and obtain NATO membership in 2023. This war has also had an important impact on Finland's implementation of the Schengen acquis, as this Member State is responsible for securing the longest EU land border section with Russia of 1 346,3 km. Hybrid challenges and evolving threats are the main elements to be addressed by the Finnish authorities responsible for the implementation of the Schengen acquis, in particular the instrumentalization of irregular migration orchestrated by Russia to Finland, which could trigger specific actions to be taken by the Finnish authorities, including possible restrictions of the cross-border traffic and closure of the border crossing points. The situation at the border between Finland and Russia is unpredictable therefore the Finnish authorities must ensure constant readiness and sufficient response capabilities. As a Baltic Sea state, the Finnish economy is highly dependent on an 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 energetic and digital disruption.

Despite the complex environment, Finland 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 with all relevant authorities involved in border control (the Customs, the Migration Authority, the National Police, the Defence Ministry). Finland delivers a reliable contribution to the European Border and Coast Guard and makes efficient use of the support provided by Europol. The overall performance of the Finnish border management system is guaranteed by the Finnish Border Guard, whose staff receives adequate basic training. Operational resilience and sufficient response capacity are ensured by efficient contingency planning and broad national situational picture provided by the implementation of EUROSUR hence were considered best practices.

The weakest element of the integrated border management in Finland is the insufficient alignment and harmonisation between the quality of border control and risk analysis performed by the Finnish Border Guard compared to the Customs and the National Police carrying out first line border checks, which in some locations results in uneven and low level

of border checks at some land, sea and air border crossing points. This also hampers the overall situational awareness requiring further integration of all national authorities involved in border control and return in the strategic planning of national capabilities. In addition, the overall situational awareness regarding returns is still not appropriate since there are important gaps in the correct collection, analysis and assessment of statistics and available information. In addition, the new methodology to analyse the operational situation developed by the National Police Board is neither shared nor used by other authorities. On top of this, the Finnish authorities cannot insert biometric data (photographs, facial images and dactyloscopic data, including fingerprints) to the Schengen Information System (SIS) alerts and the vehicles are not checked in the SIS at the border or inland.

The quality of the land border surveillance is good, but highly dependent on the operational situation at the land border with Russia. The existing capacities are sufficient only if the situation does not change as the financing for maintenance and running costs are not guaranteed and the acquisition of additional stationary and mobile means, as well as adequate increase in the number of staff are not assured. The Finnish maritime border in the Baltic Sea is far away from the main routes for irregular migration to Europe and almost no incidents were detected in the past years. The quality of the sea border surveillance carried out by the Coast Guard in the Finnish Border Guard is at a high level.

At the time of the visit, the Finnish authorities did not have reintroduced border control at any of the internal border sections.

Return activities are overall effectively implemented by the Finnish authorities, while also ensuring an adequate level of protection of fundamental rights. The national system for return is supported by adequate capabilities and resources. A seamless cooperation between the different authorities involved in the return process is ensured through dedicated IT systems, coordination frameworks and operating procedures. Further improvements are required to address internal obstacles delaying return procedures. Although part of the legal framework, Finland is currently not making use of mutual recognition of return decisions.

Finland is well advanced in law enforcement cooperation for criminal investigations, providing for sufficient capabilities. The national situational awareness and threat assessment system have been systematically developed and the data management procedures have been gradually harmonised with Europol's threat assessment. Furthermore, there are some gaps in the way Finland implements the Schengen acquis linked to the composition and structure of the single point of contact and the fact that incomplete searches are conducted in European and international systems. The new security situation has also increased the importance of demilitarised and autonomous area of Åland.

With regards to information exchange and the use of large-scale IT systems, the Schengen Information System is overall integrated in border, migration and law enforcement processes. However, the functionalities of the system should be further exploited by increasing awareness and by ensuring that the obligation to insert biometric data to SIS alerts when available at national level is implemented. Furthermore, Finland should implement all mandatory functionalities, the adequate display of all information available and the systematic consultation of the Schengen Information System when the queries are performed to national police databases either in the current search system Ulkonet or replace the system

accordingly in case implementation of the required changes in the current system are not feasible.

Measures taken by the Finnish diplomatic and consular missions in third countries on the application of the EU common visa policy are well implemented. Significant improvements have been made in this area, as Finland has remedied the serious deficiencies identified in 2018. Decisions on visa are well-founded and the new visa processing IT architecture is regarded as a best practice. However, similarly to other Member States, there are delays in granting appointments by external service providers to lodge Schengen visa applications. Furthermore, the efficiency of the examination of the visa applications is suboptimal.

Finland overall complies with the data protection requirements. Shortcomings are mainly related to the timely auditing of the national Schengen and Visa Information Systems data processing operations by the Data Protection Ombudsman, and the compliance with the required retention period of audit logs by the Ministry of Foreign Affairs. In addition, the roles and responsibilities of the data controller and processor for the N.SIS and among the N.VIS data controllers are unclear and apart from a few exceptions, data subjects can exercise their right of access in the context of Schengen Information System only in person.

Although corruption is not considered an active risk in Finland, there are still limitations in the existing institutional framework, such as the lack of a national authority legally empowered to implement anti-corruption tasks. The awareness on some anti-corruption communication tools is also low.

Overall, the Finnish authorities implemented most of the recommendations issued in 2018 Schengen evaluation, but there are still several recommendations partly implemented or under implementation.

The following strategic priority areas were established by the evaluation team taking into account the prioritised recommendations reflecting the most important findings identified in the evaluation report in relation to the overall functioning of the Schengen area.¹

On the basis of the 2023 Schengen evaluation, the priority areas for Finland are:

1/ Strengthen the **land border surveillance**, by guaranteeing a sufficient number of trained staff as well as an effective implementation of the state-of-the-art technologies, taking into account the volatile operational environment at the land border with Russia;

2/ Ensure a coherent and aligned approach to **border checks** to establish a reliable situational picture and uniform implementation of procedures by the Finnish Border Guard, the National Police and the Customs;

¹ Annex 2 to the Commission Implementing Decision contains the recommendations for remedial action aimed at addressing the deficiencies, areas for improvement and indication of priority as identified in this report under Article 20 of Council Regulation (EU) 2022/922 of 9 June 2022 on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen *acquis*, and repealing Council Regulation (EU) No 1053/2013. OJ L 160 of 15.6.2022, p.1.

3/ Close gaps in **the law enforcement cooperation** by establishing an effective Single Point of Contact and a coherent case management system; update the cooperation agreements with the neighbouring Member States to enable efficient police cooperation;

4/ **Ensure effective use of the Schengen Information System**, while guaranteeing an adequate protection of personal data, by ensuring that the obligation to insert biometric data to SIS alerts when available at national level is implemented; and

5/ Increase the efficiency of **visa processing**.

2. RECOMMENDATIONS

The 2023 periodic evaluation of Finland resulted in 80 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 **2, 5, 8, 13, 15, 18, 27, 28, 34, 38, 40, 46, 49, 56, 57, 58, 61, 62, 64, 66, 68, 70, 73, 74**, highlighted in bold, should be prioritised.

Finland is recommended to:

NATIONAL SCHENGEN FRAMEWORK

Strategic framework

1. ensure that the national quality control mechanism covers all authorities involved in border management and return; and establish a structured follow-up procedure;

National capabilities

2. **establish a comprehensive and timely overview of the human resources allocated for border control at national, regional and local levels in accordance with the national capability plan; ensure constant and sufficient number of human resources for border control according to the needs of the operational situation – [prioritised recommendation];**
3. increase participation of national law enforcement authorities (Police, Customs and Border Guard) in existing training by raising awareness on continuous **training** opportunities and developing new joint training activities;
4. establish a mechanism for monitoring and identifying current and future training needs, notably for the National Police;
5. **develop and roll-out a specialised training programme for experts involved in risk analysis in accordance with the Common Integrated Risk Analysis Model in the Finnish Border Guards, Customs and Police – [prioritised recommendation];**
6. implement regularly a tailored training for customs officers tasked to perform first line border checks at Vaalima and Nuijamaa, including on entry conditions of third country nationals, and on awareness on the relevant risks, including the current risk profiles;
7. providing refresher trainings on a regular basis on border check procedures and document examination at Tampere and Turku Airports; implement systematic advance planning and tracking of undertaken trainings; ensure that the number of staff is adapted to the developing situation;
8. **ensure that all relevant officers dealing with the Schengen Information System perform the regular mandatory refresher training on the new functionalities of the Schengen Information System – [prioritised recommendation];**

9. ensure that competent authorities provide all relevant end users of the Schengen Information System or at the SIRENE Bureau perform the regular mandatory refresher training on data security, data protection and data quality;

Functioning of the authorities

Strengthen its **anticorruption framework** by:

10. appointing a legally empowered central authority tasked with the coordination and implementation of comprehensive anticorruption measures at national level;
11. establishing a network of independent special anticorruption rapporteurs strategically placed within all law enforcement authorities;
12. raise the awareness of the new whistle blowers' protection channel within the law enforcement authorities.

Use of large-scale information systems including data protection requirements

Enhance the processes and tools for the **insertion and update of data** into the Schengen Information System by:

13. **providing in the national legislation the possibility to insert biometric data and photographs to alerts in accordance with Article 20 and 22(2) of Regulation (EU) 2018/1861, including return alerts based on Article 1, Article 4 and Article 19 Regulation (EU) 2018/1860 – [prioritised recommendation];**
14. providing for tools and training on transliteration to support end-users to enter the names in the original format for the Central System to process and prepare all variants of transliteration in a common way and improve the accuracy of search results;

Improve the **access, search, display and use of data** in the Schengen Information System by:

15. **implementing all mandatory functionalities, the adequate display of all information available and the systematic consultation of the Schengen Information System when the queries are performed to national police databases either in the current search system or replace the system accordingly in case implementation of the required changes in ULKONET are not feasible, as required by Article 9(1) of Regulation (EU) 2018/1861, Article 9(1) of Regulation 2018/1862, and Article 19 of Regulation (EU) 2018/1860, as applicable to return alerts - [prioritised recommendation];**
16. ensuring that in the RENKI application all the information in the alert is displayed to the end-users, in particular the alternative action, the type of offence and the categorisation on alerts on missing person or vulnerable person who need to be prevented from travelling, as well as the value “no” in the field “voluntary departure granted” in return alerts, whether the person is a beneficiary of the right of free movement in refusal of entry alerts in accordance with Articles 3 and 9(1) of Regulation (EU) 2018/1861 and Articles 3 and 9(1) of Regulation (EU) 2018/1862;
17. ensuring that the new queries introduced by SIS recast are implemented in the RENKI application and that related training is provided to the end-users;

18. **implementing dactyloscopy searches Common Print Search, Mark to Print, Mark to Mark against SIS AFIS in all 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. ensuring that user profiles with regards to SIS access are consistently applied;
20. ensuring that all the vehicles, accompanying vehicle registration certificates, boats, boat engines, aircrafts, aircraft engines presented to services for registration are systematically checked against the Schengen Information System prior to national registration in accordance with Articles 45 and 46 of Regulation (EU) 2018/1862;
21. integrating the national automated number plate recognition system REVIKA used by the Finnish Police with SIS;
22. ensuring that the Finnish Immigration Service checks document alerts in a systematic manner;
23. increasing the training to end-users on the actions to be taken in case of flagged and linked alerts; provide specific training on SIS to Finnish Migration Service end-users, in particular with regard to the actions to be taken and reporting hits;
24. implementing a tool for automatic collection of statistical data of the use of SIS;

Improve the **exchange of information** by:

25. improving the hit-report management, in particular by reporting hits to the SIRENE Bureau on national post-hit reporting forms which include clearly indicated mandatory fields, directly available in end-user interfaces and sent to the SIRENE Bureau in an automated way, directly from the application, in order to facilitate the exchange of information in an automated manner;(priority)
26. developing the SIRENE workflow system ADVANIA in order to facilitate automation in the case management system and in particular providing for automated checks in relation to incoming forms against national databases;

Improve the **storage of data** in the Schengen Information System by:

27. **implementing a backup of the national Schengen Information System ensuring that all national components are redundant in accordance with Article 4(1)(b) of Regulation (EU) 2018/1861 and Article 4(1)(b) of Regulation (EU) 2018/1862 – [prioritised recommendation];**
28. **formally adopting and implementing a business continuity plan and a disaster recovery plan encompassing all N.SIS components and covering all requirements in accordance with Article 10 of Regulation (EU) 2018/1861 and Article 10 of Regulation (EU) 2018/1862 – [prioritised recommendation];**
29. updating and formally adopting the existing security plan to ensure a comprehensive risk assessment of the national Schengen Information System in compliance with Article 10 of Regulation (EU) 2018/1861 and Article 10 of Regulation (EU) 2018/1862;

30. strengthening the overall management of SIS by the Finnish N.SIS Office, notably ensuring a regular and systematic reporting from Valtori of the information related to statistics about the availability and performance of all N.SIS components, overviews of all issues, incidents and maintenance operations that occurred on all N.SIS components and the N.SIS infrastructure, and all tickets and issues are addressed to eu-LISA on behalf of the Finnish N.SIS office;

Ensure the **protection of personal data** in the Schengen Information System by:

31. concluding a data processing agreement in which all responsibilities of the data processor in regard to the national Schengen Information System are clearly stated;
32. establishing the roles and responsibilities of personnel who can access and provide access to the Schengen Information System server room (TAP at the National Bureau of Investigation);
33. establishing an organisational measure to carry out regular self-auditing and self-monitoring of logs, conducting checks at a fixed interval and ensuring the development of log controls by automated means;
34. **ensuring that the exercise of data subjects' right of access to personal data in Schengen Information System is not limited to situations where it can be done in person by providing alternative options to the identification of data subjects in person, including for third country nationals, when exercising their data subjects' rights – [prioritised recommendation];**
35. ensuring that the National Police Board informs in their replies to data subjects' requests about their right to an effective judicial remedy and that this information is made available also on the National Police Board's website in a clear and easily accessible manner;
36. providing proactively information to data subjects about the processing of their personal data in the context of the Schengen Information System and the exercise of their rights at airports and police stations, orally and in printed form (e.g. flyers, posters).

Data protection supervision

Ensure that the requirements for the protection of personal data protection are fulfilled by:

37. taking measures to guarantee that data subjects exercising their rights have a right to an effective judicial remedy in case where the Data Protection Ombudsman does not act on their complaints in the required time;
38. **ensuring that the Data Protection Ombudsman carries out an audit of data processing operations in the Schengen Information System at least every four years – [prioritised recommendation];**
39. ensuring that the Data Protection Ombudsman carries out frequent inspections of a broader variety of end-user authorities with access to Schengen Information System data, covering also other data protection aspects than checking of alerts, and in particular carries out checks of National Schengen Information System logs;

40. **ensuring that the Data Protection Ombudsman carries out an audit of the data processing operations by the responsible visa/VIS authorities at least every four years – [prioritised recommendation];**
41. ensuring that the Data Protection Ombudsman carries out regular inspections of end-user authorities with access to the Visa Information System, and carries out regular checks of National Visa Information System logs;
42. ensuring that the Data Protection Ombudsman informs the data subjects in cases of indirect access whether or not any unlawful conduct has been detected, whenever revealing such information does not undermine the purpose of limiting the right of access; providing data subjects with information on their right to an effective judicial remedy on the website of the Data Protection Ombudsman in a clear and easily accessible manner.

Activities of Union bodies

43. in close cooperation with Frontex, ensure that Standing Corps when operating as members of the deployed teams can consult Union databases, the consultation of which is necessary for fulfilling operational aims specified in the respective operational plans;

EXTERNAL DIMENSION

44. take measures to ensure that visa applicants can lodge their application within two weeks from the date when the appointment was requested;
45. when assessing the financial means to cover the intended stay, take into consideration the ‘informal’ invitation/sponsorship letters along the lines of point 6.6.2. of the Visa Code Handbook and consider establishing a formal proof of sponsorship and/or private accommodation referred to in Article 14(4) of the Visa Code;
46. **increase the efficiency of the visa processing to ensure that visa applications are processed within 15 calendar days by – [prioritised recommendation];**
 - a. determining what is to be regarded as the date of admissibility (start of the processing time) and developing a tool in the national IT system to monitor the compliance with the 15 calendar days deadline;**
 - b. increasing the number of applications processed by decision-makers on a daily basis in the Service Centre and in Abu Dhabi;**
 - c. either instructing the consulates in China to pre-check the supporting documents to facilitate the decision-making in the Service Centre or ensure that staff in Kouvola responsible for examining applications lodged in China understand Mandarin and have an in depth knowledge regarding the local circumstances;**
 - d. ensuring that the decisions taken in the Service Centre are followed-up at the consulates without delay by issuing the visa or the refusal form;**

47. ensure that admissibility checks are systematically carried out, inadmissible files are always deleted from the Visa Information System and that consultations are not carried out before the applications have been deemed admissible;

Ensure the **protection of personal data** in the visa issuing procedure, including the use of the Visa Information System by:

48. clarifying the relationship between the Ministry for Foreign Affairs and all authorities with access to the National Visa Information System and their respective roles in law or an agreement;
49. **ensuring the lawful retention period for the audit logs – [prioritised recommendation];**
50. ensuring that the Ministry for Foreign Affairs informs in their replies to data subjects' requests about their right to an effective judicial remedy and that this information is made available also on the Ministry's website in a clear and easily accessible manner;
51. providing proactively information to data subjects about the processing of their personal data and the exercise of their rights, orally and in printed form (e.g. flyers, posters), at visa-issuing points;

MANAGEMENT OF THE EXTERNAL BORDERS

National and European situational awareness and early warning system

52. upload information from the national operational layer to the European Situational Picture, in particular when hosting joint operations coordinated by Frontex;
53. upload regularly risk analysis and other information in the analysis layer of Eurosur;

Risk analysis

54. improve the national risk analysis system by establishing national guidelines for risk analysis to be used by all authorities involved in border control, in particular the customs and police officers, and by taking measures to ensure that risk analysis products are produced and disseminated to all relevant officers;
55. provide the police officers responsible for border checks at airports as well as the border guards of the Crime Investigation Unit of the West Finland Coast Guard District access to all risk analysis products relevant for border checks prepared by the Finnish Border Guard; designate a person at both Tampere and Turku airports to act as a contact point for risk analysis related information exchange;

Border surveillance

56. **guarantee the necessary funding for the development of the border surveillance capabilities at the land borders (acquisition of additional equipment, modernisation of equipment and infrastructure, maintenance, running costs, swift and rapid construction of technical surveillance obstacle) in accordance with national capability development planning processes – [prioritised recommendation];**

57. **ensure and guarantee sufficient number of trained staff for land borders surveillance taking also into account potential changes of the current border situation – [prioritised recommendation];**

Border checks

58. **bring the refusal of entry procedure in compliance with Articles 3 and 14 of the Schengen Borders Code and ensure that third-country nationals refused entry do not enter Finland – [prioritised recommendation];**
59. provide police officers responsible for border checks at airports as well as the border guards of the Crime Investigation Unit of the West Finland Coast Guard District access to all relevant risk analysis products prepared by the Finnish Border Guard; designate a contact point for risk analysis related information exchange at both Tampere and Turku airports;
60. ensure sufficient command in Russian language for the border guards and customs officers performing border checks at the land border with Russia, notably by increasing the Russian language training;
61. **ensure coherent and systematic information exchange at the land borders between border guards and customs officers carrying out first line checks, by also providing regular briefings and debriefings, including commons briefing between the shift leaders of the Border Guards and Customs (Vaalimaa and Nuijamaa border crossing points) – [prioritised recommendation];**
62. **develop tailored risk analysis for physical checks of cargo and vehicle traffic; increase the number of physical controls on vehicles; increase the awareness of border guards and the customs officers on the specific risk profiles when performing border checks – [prioritised recommendation];**
63. improve the infrastructure supporting the border checks at Niirala Border Crossing Point and improve the set-up of the outside area in front of the Passenger Traffic Centre in Vaalimaa and Nuijamaa border crossing points to allow for a complete observation of the passenger flow and ensure a proper profiling of the passenger flow by the border guards;

NATIONAL RETURN SYSTEM

64. **Ensure the enforcement of return decisions in an effective and proportionate manner, in accordance with Article 8(1) of Directive 2008/115/EC particularly by – [prioritised recommendation]:**
- a. taking measures to deal in a swift manner with appeals lodged for the sole purpose of delaying or hampering a return procedure;**
 - b. accelerating return procedures, removing existing procedural obstacles, including enhancing the notification procedure of return decisions, especially in cases where the third-country national absconds,**
 - c. further enhancing the follow-up of return decisions throughout the whole return process across institutions when different case workers are involved**

in the same case, without having a complete view of the individual circumstances of the said case;

65. amend the return decisions and entry bans to clearly stipulate the obligation to leave and the prohibition to entry respectively, the territory of the European Union and the Schengen Area;
66. **ensure that, in case third-country nationals do not appeal the detention decision, reviews of prolonged detention periods are nonetheless subject to a judicial supervision to verify if the conditions for detention still exist as required by Article 15(3) of Directive 2008/115/EC – [prioritised recommendation];**
67. Enhance the effectiveness of the forced-return monitoring system by:
 - a. increasing the intensity of the physical monitoring activity;
 - b. further enhancing the provision of systematic and timely exchanging information with the Non-discrimination Ombudsman, in particular information on vulnerabilities of third-country nationals subject to a forced-return procedure;
 - c. enlarging the scope of the monitoring activities to cover all types and stages of forced-return operations (charter flights, scheduled flights, land operations to third countries;
68. **ensure that detention pending removal takes place as a rule in a specialised detention facility, including in cases of aggressive/disruptive detainees, as required by Article 16(1) of Directive 2008/115/EC; when obliged to resort to prison accommodation, adopt the necessary measures to guarantee that third country-nationals detained pending removal are kept separate from ordinary prisoners, in line with Article 16(1) of Directive 2008/115/EC - [prioritised recommendation];**
69. extend the house rules available in Joutseno Detention Centre to include information on legal aid and social support, as well as provide information explaining the rules applying to solitary confinement;

MEASURES WITHIN THE AREA OF FREEDOM, SECURITY AND JUSTICE

70. **revise all bilateral and multilateral police cooperation agreements to include provisions on operational law enforcement cooperation and to develop a formal review mechanism – [prioritised recommendation];**
71. expand the use of the new risk assessment methodology established by the National Police Board with regard to law enforcement aspects to other law enforcement authorities to establish a standardised risk assessment and analysis model for international law enforcement cooperation;
72. enhance the coordination between the National Police Board and the Police Authority of the Åland Islands, improving also the translation capacity of the National Police Board to ensure comprehensive and regular information and situational awareness for the Åland Police Authority as well as other Swedish speaking officers;

Enhance the **Single Point of Contact** by:

73. **providing for the legal and organisational integration of all national law enforcement authorities according to the Directive (EU) 2023/977 – [prioritised recommendation];**
74. **setting up a single electronic case management system, ensuring the automation of information processing, the tracking of deadlines and the monitoring of backlog, incorporating all channels of international law enforcement information exchange – [prioritised recommendation];**

Improve the **exchange of information** process by:

75. improving the hit-report management, in particular by reporting hits to the SIRENE Bureau on national post-hit reporting forms which include clearly indicated mandatory fields, directly available in end-user interfaces and sent to the SIRENE Bureau in an automated way, directly from the application, in order to facilitate the exchange of information in an automated manner;
76. developing the SIRENE workflow system ADVANIA in order to facilitate automation in the case management system and in particular providing for automated checks in relation to incoming forms against national databases;
77. develop clear and user-friendly written guidelines regarding the rules of cross-border information exchange, choice of international police cooperation tools and communication channels (listing for instance practical examples);
78. establish clear modalities to ensure efficient implementation and full awareness of the access procedure for law enforcement purposes to the Visa Information System;
79. 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;
80. improve the use of the Europol Information System by expanding the technical solution for uploading data to include all types of data with operational value.