



# Schengen Evaluation of **CROATIA**

EXECUTIVE SUMMARY &  
RECOMMENDATIONS



# SCHENGEN EVALUATION OF CROATIA EXECUTIVE SUMMARY AND RECOMMENDATIONS

## 1. EXECUTIVE SUMMARY

A Schengen evaluation of Croatia was carried out in the period December 2023 – February 2024 by Commission and Member State experts accompanied by observers from relevant Agencies and bodies<sup>1</sup>. 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 2024 Schengen evaluation of Croatia.<sup>2</sup>

On 1 January 2023 Croatia became a full member of the Schengen area, marking an important milestone in the history of both Croatia and the European Union. Their Schengen accession followed a period of intensive preparation and substantial efforts to meet all the necessary requirements for the full application of the Schengen acquis. Since the accession, Croatia has been facing an increase in cross-border crime and migratory pressure at its external land borders, especially at the Bosnia and Herzegovina – Croatian - Slovenian corridor, which subsequently had an impact on neighbouring and other Member States with an increase in secondary movements. The main challenges to be addressed by the Croatian authorities responsible for the implementation of the Schengen acquis are the detection of cross-border crime and irregular migration, the registration of irregular migrants and ultimately the prevention of secondary movements to other EU Member States.

Notwithstanding the challenges it has been facing after its Schengen accession, **Croatia is overall effectively, efficiently and correctly implementing the Schengen acquis**, and thereby actively contributing to the well-functioning of the Schengen area. There are however concerns related to the level of implementation of the data protection part of the acquis, which is considered insufficient.

Croatia has a well-established and functional European integrated border management, based on a national strategy. There is a clear chain of command, coordination, and effective cooperation between the authorities responsible for border management. The efficient governance of the European integrated border management is supported by a well-established national risk analysis system, functional quality control mechanism and coherent data collection for vulnerability assessment. The systematic gathering of information results in a comprehensive national situational picture and awareness and serves as a basis for various

---

<sup>1</sup> The European Border and Coast Guard Agency (Frontex), Europol, eu-LISA, the European Union Agency for Fundamental Rights and the European Data Protection Supervisor.

<sup>2</sup> The report contains findings and recommendations for remedial actions as well as detailed information concerning the on-site visits carried out between December 2023 and February 2024 (enclosure 1) and on national authorities responsible for the implementation of the Schengen acquis in various fields covered by this report (enclosure 2).

risk analysis products. Furthermore, Croatia delivers a reliable contribution to the European Border and Coast Guard (EBCG), while also making efficient use of EBCG capabilities in the areas of border checks and return (e.g., Frontex Joint Reintegration Services), however support for border surveillance activities has so far not been requested.

The quality of the sea and land border surveillance carried out by the Border Police is at an adequate level, however, the fact that Croatia remains affected by increased migratory pressure creates the necessary challenges in the management of external land borders. This is seen in particular at the border with Bosnia and Herzegovina where the coverage of the stationary surveillance capacity was assessed as low at the time of evaluation, while the number of canine units and border guards to efficiently counterbalance this deficiency were limited. Croatia has been mitigating the identified challenges by continuously procuring additional technical equipment and by investing in additional human resources required for an efficient and effective response to all threats at the external borders. Croatia has underlined its commitment to continue strengthening its land border surveillance, in particular at the border with Bosnia and Herzegovina. The border checks at the air, land and sea borders are adequate, although improvements are necessary in the thorough check of third country nationals. Moreover, the lack of effective control of pleasure boats poses a threat to tackling the smuggling of irregular migrants and other cross-border crime and could eventually lead to encouraging the establishment of irregular migration routes.

The current level of human resources for police, return and border control tasks is sufficient. However, the allocation of posts and distribution of staff are not sufficiently adjusted to the changes in the workload, new tasks, and the operational situation (risks and threats) that have occurred after Croatia's Schengen accession. Moreover, Croatia does not have multi-annual human resources strategies for the Police and Border Police.

Particular attention was paid to verifying the respect of fundamental rights with some specific practices identified having a negative impact on certain fundamental rights, but also a best practice related to the training system on fundamental rights. Overall, the Croatian authorities duly consider fundamental rights when implementing the Schengen acquis and Croatia established an independent monitoring mechanism related to fundamental rights compliance by border guards at the external borders. The most important elements for improvement are the current lack of an Independent Forced Return Monitoring Mechanism, the lack of systematic consideration of non-refoulement in the return and readmission procedure and the limited access to legal remedies.

The Croatian implementation of the Schengen acquis in the field of return is well established, with a clear division of tasks of authorities involved, national strategies, contingency planning and access to the relevant financial instruments being in place. The current and planned human resources are adequate for the current caseload, however they prevent a proactive approach to issue return decisions to any illegally (over)staying third country nationals. To this end, inter-agency cooperation should be enhanced including through further developing the Information System of the Ministry of the Interior. Taking all necessary

measures to enforce removal needs improvement, in full respect of the principle of *non-refoulement* and the suspensive effect to removal in such appeal cases.

It must also be noted that the Croatian return system relies largely on bilateral readmission agreements with its neighbouring countries, creating a situation where repeated attempts of illegal entry from the same third country national are common. Returns to countries of origin of third country nationals (forced or voluntary), coupled with broader reintegration assistance possibilities could contribute to a more sustainable return of third country nationals.

The current detention capacity is sufficient, given the average short duration of detention of third country nationals. The outdoor recreational areas both for adults and young children offer good conditions for activities and privacy.

As far as the implementation of the EU visa *acquis* is concerned, Croatia complies with the Visa Code and other relevant legislation. The examination of the applications is solid, and decisions are well-founded at the visited consulates in Istanbul and Pretoria. The IT system is user friendly and functioning well. It has innovative and intuitive functionalities to support the examination process, e.g., on security features of travel documents. The staff is well trained in the use of various tools to detect forged documents and is making full use of them. The shortcomings identified include the excessive mandatory two-way courier fee charged in many locations by the external service provider under the contract with the Croatian Ministry of Foreign and European Affairs. In numerous countries Croatia has neither consulates nor is represented by another Member State, which poses challenges for both the applicants and consulates, the latter in terms of monitoring burden.

Large-scale IT systems supporting the well-functioning of the Schengen area, notably the Schengen and Visa Information Systems, are adequately implemented. The Schengen Information System (SIS) and SIRENE procedures are well integrated in the border, migration and law enforcement processes in Croatia. There is a very high level of automation of processes ensuring that the Schengen Information System is systematically searched, including several best practices, such as the automated systematic check of all vehicles in incoming customs declarations and the automated pre-check of all vehicles in the Schengen Information System via the Automatic Number Plate Recognition at the land borders. All these aspects contribute to ensuring a high level of security in the Schengen area. However, further improvements should be made to ensure a more effective use of the Schengen Information System, in particular the implementation of dactyloscopic searches in the SIS-AFIS, as well as the systematic attachment of fingerprints to the Croatian alerts, the performance of the mobile application and the necessary additional human resources to be provided to the SIRENE Bureau following Schengen accession and in view of the upcoming tasks related to ETIAS, VIS, Interoperability, new alerts and the need to provide further training to other authorities.

The Croatian internal security system is well-established, intelligence-driven and based on very effective and clearly regulated and implemented interagency cooperation between all law enforcement authorities. The national strategic framework, governance and respective

strategies for internal security are based on threat assessment and are well connected to the implementation of the EU priorities and the recommendations of the Schengen evaluation. The security situation at the internal border with Slovenia was a source of concern during the evaluation, due to increasing numbers of irregular migrants entering Croatia at the external borders, in particular through the Bosnia and Herzegovina - Croatian land border and exiting the country to Slovenia without being properly detected and checked, as well as the increasing risk of other cross border crime at the internal border. At the time of the visit, Slovenia had reintroduced border control with Croatia. Despite some developments and use of compensatory measures, the implementation of the cross-border cooperation with Slovenia does not correspond to the new operational situation. This is partly due to the lack of an up-to-date bilateral agreement with Slovenia, but also due to the limited use of existing instruments (hot pursuit, joint patrols, and capacity of Police and Customs Centres), as well as the lack of a comprehensive cross-border cooperation concept combining all available instruments. A point of concern is also the very limited capacity to consult national and international databases by police patrols due to the lack of mobile devices connected to national and international databases.

As regards data protection, Croatia was assessed to insufficiently comply with the Schengen acquis. In particular, the Croatian Data Protection Authority (DPA) and the Independent Department for Supervision of Personal Data Protection of the Ministry of the Interior (which includes the Data Protection Officer) are not adequately engaged in the supervision and enforcement of data protection rules in the Schengen and Visa Information Systems. What is more, the roles and responsibilities within and between different authorities are unclear. As a result, the principle of accountability is not respected and self-monitoring of compliance with data protection rules is not adequate. Furthermore, police officers are unaware of the possibility to address and direct data subjects towards their data protection officer.

On the basis of the 2024 Schengen evaluation, the priority areas for Croatia are:

- ✓ Strengthen the border surveillance capacity at the land border with Bosnia and Herzegovina, providing a sufficient number of trained staff, including dog units at high-risk areas, and stationary surveillance capacity.
- ✓ Establish a comprehensive multiannual human resources strategy for Croatian law enforcement authorities (Police and Border Police).
- ✓ Ensure the entry of fingerprints to the Schengen Information System (SIS), also in view of interoperability and the full use of fingerprint searches in the SIS; as well as further improve the relevant end-user applications to ensure that all of search functionalities of the SIS are implemented and produce a result equivalent to that of a search in the SIS database, displaying all available information.
- ✓ Strengthen the cross-border police cooperation with the neighbouring Member States by 1) revising the bilateral agreement with Slovenia; 2) developing and putting into practice a comprehensive concept combining all available instruments (Police Cooperation Centres, joint operations, risk analysis, joint investigations, etc.), and 3) increasing the number of mobile devices to be used by police patrols.

- ✓ Ensure properly defined roles, responsibilities, and data controllership arrangements between different authorities managing and using EU large-scale IT systems.

## 2. RECOMMENDATIONS

The 2024 periodic evaluation of Croatia resulted in 114 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 2, 4, 8, 14, 24, 34, 36, 48, 52, 56, 57, 62, 82, 101 and 107, highlighted in bold, should be prioritised.

Recommendations number 46, 47 and 83 relate to persistent deficiencies which have already been identified in the first time Schengen evaluation of Croatia.

Croatia is recommended to:

### NATIONAL SCHENGEN GOVERNANCE

#### National strategies and quality control mechanisms

1. ensure that the implementation of the Schengen acquis and the recommendations of the Schengen evaluation process are adequately included and prioritised in when updating the Implementation Programme related to national internal security;

#### National capabilities

2. **establish a comprehensive long-term human resources strategy for the Police and the Border Police, including revision of the recruitment criteria for the Police, and develop a system for regular monitoring of the staffing needs at the regional and local level;** (*prioritised recommendation*)
3. reassess the current allocation of posts and distribution of trained staff of the:
  - a. Border Police, by taking into account the operational environment, results of risk analysis and forecasting (i.e on passenger and migration flows), in particular in the areas with persistent migration pressure and optimise the use of staff by redeployment to these areas;
  - b. Police, by focussing on the core police functions, including return, foreseeing future developments and allowing for *possible optimization*;
4. **ensure the increase in staffing for the SIRENE Bureau and the Single Point of Contact;** (*prioritised recommendation*)
5. increase the capacity to perform the basic training of 8 weeks for the Border Police and ensure that the regular basic, specialised and refresher training on border control is mandatory and aligned in all border police administrations and border police stations;
6. implement sufficient training for border guards in screening and debriefing at regional and local level, as well as in cultural awareness and language skills for those dealing with third country nationals in return procedures and working in detention centres;

7. ensure mandatory training for all authorities with access to the SIS, comparable to the police SIS training, including training on the system of automated transfer of personal data from national alerts to SIS and access rights, data protection and security, and involve the Croatian data protection authority and the data protection officer of the Ministry of the Interior in planning and evaluation of those trainings;
8. **ensure specific training of all police officers and border guards on Article 36 alerts (discreet check alerts, Regulation (EU) 2018/1862), specifically targeting national and regional units involved in the investigation of crime in relation to the use of Article 36 alerts and all end-users, on how to correctly carry out the actions to be taken;** (*prioritised recommendation*)
9. ensure proper training and common awareness to all end-users of the Visa Information System on data protection and data security;
10. further develop and deliver well-structured and practice-oriented, sufficiently detailed training for border guards on how to detect (potential) victims of trafficking in human beings and how to systematically refer them to appropriate procedures, including regular specialised refresher courses.
11. establish a structured framework for obligatory and certified international law enforcement cooperation training for all involved authorities both in basic and continuous training curricula, with particular emphasis on international and EU databases, cross-border cooperation, and other Schengen-related matters, further employing online training modality and ensuring better use of CEPOL instruments. Promote English language training, especially among the employees performing the functions of the international dimension;
12. develop dedicated continuous training as well as a system to evaluate training effectiveness for the staff of the Single Point of Contact;
13. increase the number of service dogs and dog handlers for land border control;
14. **increase the capacity of the Police to conduct direct searches in national and international databases by increasing the number of mobile devices to be used by police patrols (including during joint patrols with neighbouring countries) and ensure that all police officers are trained to make use of all the functionalities of their mobile devices;** (*prioritised recommendation*);
15. update the National Contingency Plan in accordance with the Handbook on Contingency Planning for Border Management, and test it regularly;
16. revise the national contingency plan and prepare the relevant chapters together with Frontex and with the neighbouring Member States as required by Article 9, paragraph 5 of Regulation (EU) 2019/1896;

### **Functioning of the authorities**

17. further strengthen the commitment to combat corruption and promote ethics and integrity among the employees of the law enforcement authorities by conducting a comprehensive risk assessment of corruption-prone areas and taking appropriate measures to overcome the detected deficiencies, providing employees with clear definitions, guidelines and examples to guide their behaviour, ensuring the provision of formalized training on the

subject matter and raising the employees' awareness on the possibility of anonymous reporting and activity of Ethics Commissioners.

18. regularly monitor the index of inhabitants' satisfaction (trust level) with the services of its law enforcement authorities by procuring independent surveys of the subject matter.

### **Fundamental rights**

19. ensure that risks of *refoulement* and vulnerability are systematically assessed prior to taking a decision on return or readmission;
20. ensure to always hand over the notification form (No. 11) to every apprehended third-country national in an irregular situation who is subjected to readmission or return; and provide sufficient information orally before proceeding with the readmission or return;
21. set up an effective forced-return monitoring system in accordance with the requirements of Article 8(6) of the Return Directive;
22. ensure the effective financing for the sustainable functioning of the Independent Monitoring Mechanism on the Protection of Fundamental Rights in Action of Police Officers and to guarantee the implementation of regular announced and unannounced monitoring visits and timely setting up and running of the mechanism's website, also further reflecting the general guidance of the European Union Agency for Fundamental Rights into its operation;
23. increase the effectiveness and number of investigations initiated by the authorities on their own (*ex officio*) into allegations of ill-treatment by the border police at external borders;

### **Large-scale IT systems – Schengen Information System (SIS)**

24. **ensure automation of attaching fingerprints from all national source systems to all alert categories on persons;** (*prioritised recommendation*)
25. establish the legal and technical possibility to enter alerts on vulnerable adults who need to be prevented from travelling;
26. ensure the deletion of alerts on return without delay following the receipt of the confirmation of return outside office hours and where applicable, enter the alert for refusal of entry and stay without delay in accordance with Articles 6(2), 8 of Regulation (EU) 2018/1860 and Article 24(1)(b) of Regulation (EU) 2018/1861;
27. ensure that all available information of a return alert, including updates concerning a suspension or postponement is uploaded to the SIS alert without any delay in accordance with Article 3(5) and Article 4(2) of Regulation (EU) 2018/1860;
28. ensure that the photo is attached to the return or entry ban alert when available in accordance with Article 4(1)(u) of Regulation (EU) 2018/1860 and Article 20(3)(w) read in conjunction with Article 22(1) of Regulation (EU) 2018/1861;
29. raise awareness on the operational advantages of linking alerts, ensure that the links between national alerts are also available in the Schengen Information System and implement the use of links also in relation to discreet checks alerts;



30. ensure that, in case of warning of duplicated record from Central SIS, the record is deleted from the SIS in accordance with Article 23(2) of Regulation (EU) 2018/1862 and Regulation (EU) 2018/1861;
31. improve the data quality control procedure by including periodic double checks, especially in the wanted person category;
32. ensure that the service responsible for issuing registration certificates for boats has access to the full data set stored in SIS and include in the internal procedure that in case of a hit the Police are informed in accordance with Article 46 of Regulation (EU) 2018/1862;
33. ensure that the services responsible for issuing registration certificates for firearms shall have access to data on persons entered in SIS in accordance with Article 47(1) of Regulation (EU) 2018/1862;
34. **ensure that the fingerprint queries can be carried out easily and are broadly available and used;** (*prioritised recommendation*)
35. ensure that in the Ministry of the Interior application, all data available in any SIS alert is always displayed to the end users in case of a hit on alerts on refusal of entry and stay in accordance with Article 9(2) of Regulation (EU) 2018/1861;
36. **ensure that in the Ministry of the Interior application all of the search functionalities of the SIS are implemented in accordance with Article 9(2) of Regulation (EU) 2018/1861 and Article 9(2) of Regulation (EU) 2018/1862;** (*prioritised recommendation*)
37. improve the display of information in the Ministry of the Interior application by highlighting information or considering the use of icons/symbols;
38. further develop the mobile application and ensure that the searches carried out produce a result equivalent to that of a search in the SIS database in accordance with Article 9(2) of both Regulation (EU) 2018/1862 and Regulation (EU) 2018/1861;
39. further develop the mobile application to ensure the direct opening of the links (and the subsequent display of all the alert data of the linked alert including the photo), the highlighting of immediate action and the prominence of the information concerning the misused identity;
40. ensure the deletion of supplementary information at the latest one year after the related alert has been deleted from SIS in accordance with Article 64(2) of Regulation (EU) 2018/1862 and Article 49 (2) of Regulation (EU) 2018/1861;
41. ensure that the SIRENE channel is systematically used for exchange of supplementary information on SIS alerts pursuant to Article 8(1) of Regulation (EU) 2018/1862 and Article 5 of Commission Implementing Decision C (2021)7901 final (SIRENE Manual - Police);
42. improve the structure of the hit reporting form to ensure that all information reflecting the content of G, H and R forms are provided;

### **Protection of personal data in the Schengen Information System**

43. ensure that an efficient system of SIS user registration review is carried out regularly;

44. implement a specific policy covering the use of computers or other mobile devices (with access to SIS) outside the Ministry of the Interior network in accordance with Article 10(1)(k) of Regulation (EU) 2018/1862;
45. ensure that checks of accuracy and legality of alerts are introduced in the procedure of entering all SIS alerts. In particular, a review of the national alerts created before 2017 is necessary to ensure there are no outdated alerts in the SIS;
46. ensure that the Ministry of the Interior internal procedures on personal data breaches in relation to the use of the SIS are correctly applied, by documenting any personal data breach, including their effects and remedial action taken and notifying data breached to the DPA and/or affected data subject. Conduct regular reviews (by the DPA) to ascertain these procedures are put in place and practice <sup>3</sup>;
47. ensure regular and systematic log files audit to determine the lawfulness of data processing carried out in N.SIS by end-users by the Ministry of the Interior and Data Protection Authority, including by adopting appropriate policies in accordance with point 1 of Article 10 (self-auditing) and Article 12 of Regulation (EU) 2018/1862<sup>4</sup>;
48. **put the necessary technical and organisational mechanisms in place to ensure automatic, regular and systematic checks of the SIS log files by the Ministry of the Interior;** (*prioritised recommendation*)
49. ensure that retention periods are respected for both electronic and paper files, in accordance with Articles 57 and 64 of Regulation (EU) 2018/1862;
50. ensure that a proper user authentication and user control mechanism is in place when accessing TETRA radio communication stations, in accordance with Article 10(1)(e); ensure that every access to and all exchanges of personal data within SIS are logged in accordance with Article 12 of Regulation (EU) 2018/1862;
51. ensure that computer workstations operated by the SIRENE Bureau which have direct access to the SIS and SIRENE are isolated either by physical network infrastructure or by virtual electronic means;
52. **ensure that the Data Protection Officer of the Ministry of the Interior reports directly to the highest level of management and is given the required independence to perform his/her tasks as provided for in Articles 32 to 34 of the Directive (EU) 2016/680 and Article 38 of the Regulation (EU) 2016/679;** (*prioritised recommendation*)
53. inform data subjects about the possibility to exercise their rights through the Data Protection Agency in accordance with Article 17 of Directive (EU) 2016/680;
54. inform data subjects about the right to seek judicial remedy where they consider their rights to be infringed in the context of the SIS in the standard forms provided by the Ministry of the Interior, on the website of the Ministry, and in the replies sent by the Ministry to data subjects.

---

<sup>3</sup> Former recommendation 14 of Council Implementing Decision 5725/17 of 27.01.2017.

<sup>4</sup> Former recommendation 16 of Council Implementing Decision 5725/17 of 27.01.2017.

## **Data protection supervision**

55. guarantee full budgetary independence of the Data Protection Authority by ensuring that it is visible to the parliament which budget the DPA requested, and that the DPA has the opportunity to influence the decision on its budget when the Ministry of Finance makes amendments to its proposal before submittal to the parliament;
56. **ensure that all authorities having access to SIS are supervised by an independent data protection authority;** *(prioritised recommendation)*
57. **ensure that the Data Protection Authority carries out at least every four years an audit of data processing operations in the N.SIS, in accordance with Article 69(2) of Regulation 2018/1862, Article 55(2) of Regulation 2018/1861 and Article 19 of Regulation 2018/1860, and in the N.VIS in accordance with Article 41(2) of Regulation (EC) No 767/2008 and Article 8 (6) of Council Decision 2008/633/JHA;** *(prioritised recommendation)*
58. ensure that the Data Protection Authority carries out checks on N.SIS and VIS logs on a regular basis and not only in case of suspected problems or complaints;
59. ensure that the Data Protection Authority informs data subjects about their right to seek a judicial remedy against its decisions issued in the context of SIS;

## **Activities of Union agencies and bodies**

60. ensure, in close cooperation with Frontex, that the standing corps officers when operating as members of the deployed teams have access to consult Union and national databases relevant to the implementation of their tasks;

## **EXTERNAL DIMENSION**

### **Cooperation with third countries**

61. strengthen the national coordination concerning the deployment of law enforcement liaison officers and make full use of Council Decision 2003/170/JHA;

### **Visa and data protection**

62. **ensure without delay that visa applicants are charged only one mandatory fee (i.e., the ‘service fee’) by the external service provider at all locations (including Abuja), which complies with the maximum amount set out and in accordance with Article 17 of Regulation (EC) No 810/2009 (Visa Code);** *(prioritised recommendation)*
63. ensure that the consulate in Abuja has a clear understanding of what has to be paid by the visa applicants in Nigeria;
64. ensure that the contract with the external service provider is compliant with all the elements set out in Annex X of the Visa Code and Article 28 of the Regulation (EU) 2016/679;
65. intensify the efforts to conclude representation arrangements to increase possibilities to apply for Croatian short-stay visas and revisit all the legal possibilities to facilitate speeding up and simplifying the process;

66. consider joint monitoring activities with other Member States to ensure effective monitoring of external service providers;
67. ensure that the content of the application form to be filled-in online corresponds to the latest version of the uniform application form set out in Annex 9 of Visa Code Handbook;
68. waive the strict requirement for a formal Letter of Guarantee whenever the applicant presents credible proof of sufficient own means of subsistence and an invitation letter from the host that substantiates in a credible and verifiable manner the purpose of travel and revise the requirements for the guarantee letter so that they are in accordance with Article 14(4)(a) of the Visa Code;
69. ensure that students who intend to stay in Croatia for more than 90 days are always issued with a long-stay authorisation and not short-stay visas;
70. establish a written procedure on how to deal with data protection matters, including the requests for the exercise of data subject's rights, in the Visa Information System by the Ministry of Foreign and European Affairs and the Ministry of the Interior. Make this procedure transparent to the data subjects;
71. ensure that there is no conflict of interest in fulfilling the role of the Data Protection Officer of the Ministry of Foreign and European Affairs;
72. delete user identities of N.VIS users that left or changed roles within the Police or left the Ministry of Foreign and European Affairs in accordance with Article 36(a) of Regulation (EU) 676/2008;
73. conduct systematic checks of user rights of VIS on a regular basis to ensure the operational security of the visa information system;
74. ensure the security of the N.VIS by implementing two-factor authentication to access N.VIS;
75. inform data subjects about the right to seek judicial remedy where they consider their rights to be infringed in the context of the Visa Information System in accordance with Article 36(a)(2) and Article 38(7) of Regulation (EC) 767/2008, in conjunction with Article 79(1) of Regulation (EU) 2016/679. Such information should be included in the standard forms provided by the Ministry of Foreign and European Affairs, on the website of the Ministry of Foreign and European Affairs, and in the replies sent by the Ministry of Foreign and European Affairs to data subjects;

## **MANAGEMENT OF THE EXTERNAL BORDERS**

### **National and European situational awareness, early warning system and risk analysis**

76. bring the function of the National Coordination Centre in accordance with Article 24(1)(c) of Regulation (EU) 2019/1896, by uploading analytical products to the analytical layer of the national situational picture;
77. enhance the alignment of the EUROSUR border sections with the regional and local organisational structures and areas of responsibilities, in cooperation with Frontex;

78. systematically integrate the vulnerability as identified in the course of the analysis process in all risk analysis products at the national, regional and local level;
79. ensure that information regarding migration cases and trends from neighbouring countries is provided to the regional and local level and establish a system to estimate the number of undetected incidents and migration cases at the border to measure the permeability of the border sections to establish a complete situational awareness;

### **Border Surveillance**

80. integrate all available sensors as well as the position of patrols into a single Border Management System at the national, regional and local level;
81. adapt the integrated land border surveillance concept to increase situational awareness and detection capability by: increasing the number of stationary surveillance systems with long range day/night cameras and radar; improving the positioning of the detection equipment; prioritising the realisation of these stationary surveillance systems according to risk analysis in a ‘national land border surveillance capability enhancement plan’;
82. **urgently strengthen the land border surveillance system at the border with Bosnia and Herzegovina in accordance with Article 13 of Regulation 2016/399 to increase the situational awareness and detection capabilities, by increasing the stationary surveillance at all border sections with Bosnia and Herzegovina; as well as improving the positioning of the equipment in accordance with the risk analysis; (prioritised recommendation)**
83. establish visible border signs and border markings at the land border, as well as make the border line visible to ensure efficient implementation of the border surveillance system. finalize and further develop the integrated land border surveillance system.<sup>5</sup>;
84. establish an integrated planning of patrolling activities for sea border surveillance purposes encompassing all involved authorities in order to improve situational awareness at the sea borders;
85. integrate the Neum Corridor surveillance system in the national sea border surveillance system to have a complete and integrated maritime situational picture;
86. improve the visual coverage of the northern and central part of the maritime border during the night by upgrading the cameras along the entire borderline with night vision capability and ensure that the running and maintenance costs can be covered at all times;
87. adapt the allocation of patrol vessels and boats for each border section to the operational situation and risks related to external border management;

### **Border Checks**

88. improve the quality of border checks by ensuring proper use of document examination equipment and checking for clandestine entry at the land border crossing points; conduct

---

<sup>5</sup> Former recommendation 13 of Council Implementing Decision 13902/18 of 6 November 2018 and former recommendation 4 of Council Implementing Decision 11022/20 of 22 December 2020.

second line checks at a dedicated location separated from the first line checks at Zagreb Airport;

89. ensure that all conditions of entry are systematically checked at Zagreb airport for all third country nationals arriving in Croatia in accordance with Article 8(3) of the Schengen Borders Code;
90. ensure that external borders may only be crossed at border crossing points as required by Article 5 of the Schengen Borders Code;
91. bring the procedure of checking persons on board of pleasure boats in conformity with Article 8 and Article 19 in conjunction with Annex VI, point 3.2.4 of the Schengen Borders Code;
92. improve the display of information in the National Border Management Information System application in a user-friendly way;
93. improve the National Border Management Information System application to display all data available in the SIS alerts in accordance with Article 9(2) of Regulation (EU) 2018/1861;

#### **NATIONAL RETURN SYSTEM**

94. amend the national legislation to ensure that in case of illegal stay, third country nationals are not issued a fine instead of a return decision, in line with Article 6(1) of Directive 2008/115/EC;
95. enhance the IT tools available to police officers to increase the efficiency of return, including pro-active case handling;
96. ensure that all necessary measures are taken to ensure the enforcement of return;
97. state in all return decisions issued to illegally staying third-country nationals the obligation to leave the territory of all states of the Schengen area in order to reach a specific third country', in accordance with Articles 3(3) and 3(4) of Directive 2008/115/EC; take measures to ensure that, when the third country of return has not been specified in the return decision due to the impossibility to identify one in accordance with national law or national legal practice, the principle of non-refoulement is respected;
98. amend the national law to ensure appeals against a return decision have a suspensive effect when the enforcement of that decision may violate the principle of *non-refoulement*, in accordance with Article 13 of the Return Directive, interpreted in conjunction with Articles 5 and 9;
99. ensure clear information and wider possibility to obtain legal advice, representation and, where necessary, linguistic assistance, in compliance with conditions set by Article 13(3) of the Return Directive, in order to ensure effective remedy as envisaged Article 13(1);
100. ensure that the state of repair of the shower room and toilets in the Reception Centre for Aliens Ježevo, meet the requirements as stated in Council of Europe Guideline 10.2 and European Committee for the Prevention of Torture and Inhuman or Degrading

Treatment or Punishment (CPT) -standards on immigration detention, paragraph. 29;

## **MEASURES WITHIN THE AREA OF FREEDOM, SECURITY AND JUSTICE**

### **Exchange of information for cross-border and international police cooperation**

101. **assess and optimise the organisation and workflows of the Single Point of Contact (SPOC) as well as the tasks assigned to the SPOC staff and ensure that the Single Point of Contact is provided with the appropriate operational tools, and capabilities, necessary to carry out its tasks in an adequate, effective and rapid manner;** (*prioritised recommendation*)
102. improve the case management system for the Single Point of Contact with the increase of automation of information processing, by:
  - a. including the function to generate statistics and records in an automated manner;
  - b. including 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;
  - c. integrating Europol's Secure Information Exchange Network Application (SIENA) for incoming and outgoing messages;
  - d. setting deadlines to reply to messages and the display of the urgency of the SIRENE incoming forms;
103. improve the procedure for the designated law enforcement authorities to consult the Visa Information System for the purposes of the prevention, detection, and investigation of terrorist offences and of other serious criminal offences as envisaged by Council Decision 2008/633/JHA and raise awareness for all relevant staff on the use of Visa Information System for law enforcement;
104. ensure processing of personal data obtained from the establishments providing accommodation by competent authorities for law enforcement purposes in accordance with Article 45 CISA and the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, including by establishing proportionate retention period and access control;

### **Operational cross-border police cooperation**

105. establish a comprehensive and well-coordinated national concept for operational cross border police cooperation covering all compensatory measures within the country, in border areas and with neighbouring Member States. Development of this concept should be adequately resourced and connected to relevant strategies and EU funding programmes and it should contain regular exercises with other Member States.
106. develop a formal review mechanism for bilateral and/or multilateral agreements with the aim to increase their operational effectiveness and include provisions on operational law enforcement cooperation as envisaged by the Council Recommendation (EU) 2022/915 on operational law enforcement cooperation. Priority should be given to the already negotiated bilateral agreement with Slovenia;

107. **establish clear national procedures on the use of cross-border operations, such as hot pursuit and cross-border surveillance, raise police officers' awareness on the subject matter and organise periodic common exercises with the neighbouring Member States. The bilateral police agreement with Slovenia on cross-border cooperation, including hot pursuit, should be urgently adopted and implemented to meet the current operational needs;***(prioritised recommendation)*
108. further develop the use of joint patrol by giving officers clear orders and instructions concerning their competencies and by equipping them with mobile devices connected to national and international databases; assess the need for deployment of joint patrols with the neighbouring countries, in particular Hungary and Serbia, taking into account the operational needs;
109. ensure the interoperability of cross-border radio telecommunication and secure information exchange tools in partnership with the neighbouring countries, in accordance with Article 44 of the Convention Implementing the Schengen Agreement (CISA) and prepare the technology, application and procedures for the use of the EU Critical Communication System within the BroadEU.net.;
110. further develop the national Police Cooperation Centre (PCC) concept in order to facilitate, support, and, where relevant, coordinate joint patrols and other joint operations, connect PCCs to SIENA together with their integration into the SPOC case management system, and strengthen the national coordination mechanism e.g., by nominating a national Police and Customs Cooperation Centre' coordinator;
111. establish a clear national system to assess the overall needs for long and short-term deployment of liaison officers to other Member States;

### **Cooperation with Europol**

112. effectively utilize the available SIENA access rights by the central police entities and further roll out SIENA to the regional level as well as to the PCCs as envisaged by Directive (EU) 2023/977;
113. implement a fully automated data loader to the Europol Information System (EIS) and upload information on Croatian nationals and objects to EIS;
114. introduce a business-to-business system interface (QUEST) and adequate training for frontline investigators, criminal intelligence officers and analysts to search and access Europol's data using their national information systems.