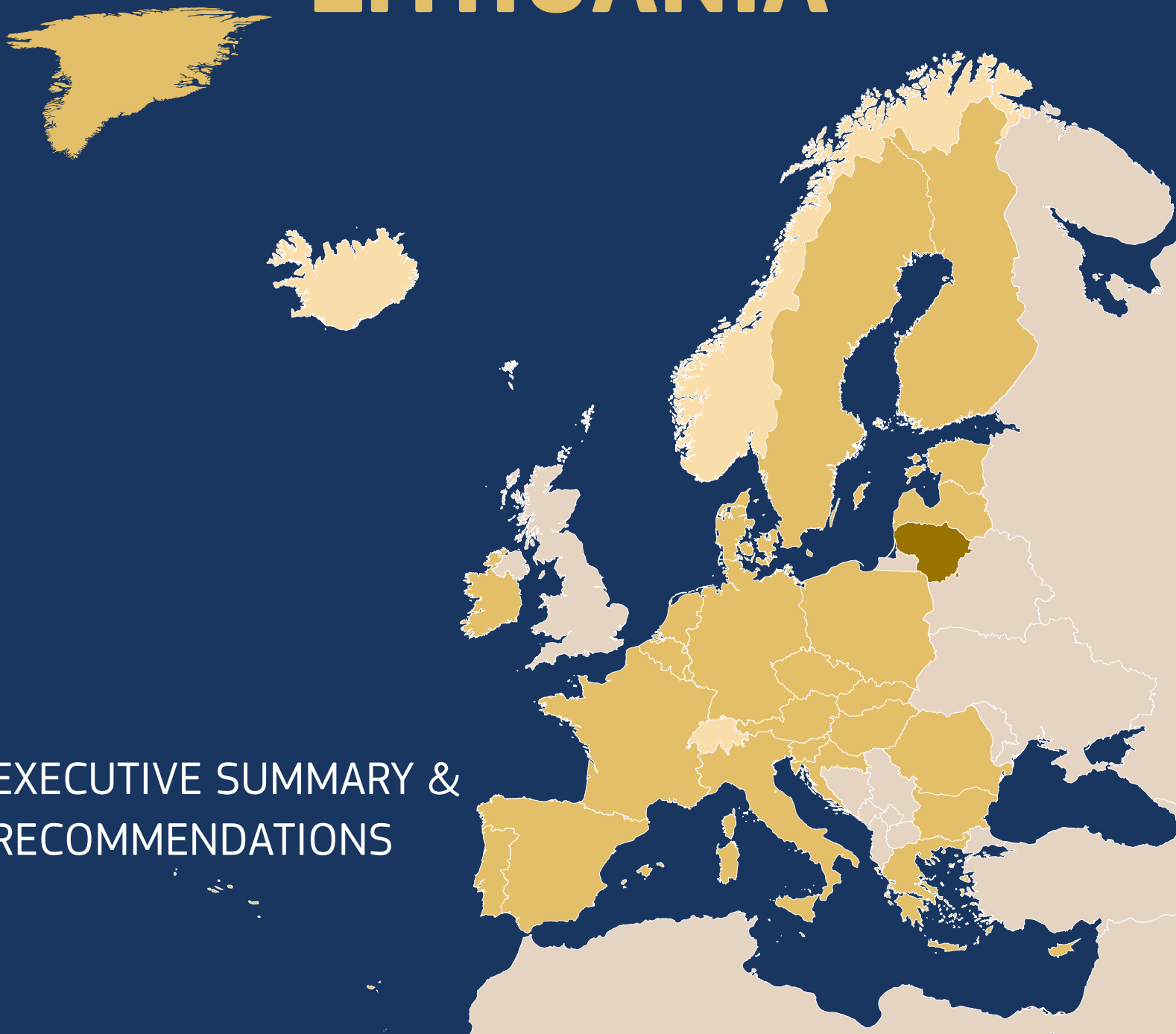
European Commission

Schengen Evaluation of **LITHUANIA**



EXECUTIVE SUMMARY & RECOMMENDATIONS

SCHENGEN EVALUATION OF LITHUANIA

EXECUTIVE SUMMARY OF THE 2023 COUNTRY REPORT

&

RECOMMENDATIONS

1. EXECUTIVE SUMMARY

Over the past two years, Lithuania has been facing significant challenges at its external borders, following the **instrumentalisation of migration by the Belarussian regime in 2021**. In July 2021, Lithuania experienced a **historic high level** in numbers of irregular border crossings (from 119 in 2019 and 121 in 2020 to 4 395 in 2021[1]). These developments severely impacted the Lithuanian border management system, which was not designed to deal with such levels of pressure. During this period, Frontex implemented a Rapid Border Intervention and provided support in organising voluntary returns. The Lithuanian authorities took immediate measures to reinforce the external border with additional staff, enhanced border surveillance infrastructure, and also established a joint investigation cell as a National Task Force. The legal framework was also amended, and measures were introduced to accelerate returns. The overall performance of **border control** and resilience during crisis situations in Lithuania is currently at high level. However, the number of staff is at the minimum level to ensure sufficient implementation of border management and return activities, and any possible change in the current situation would put under pressure the reaction capacities for border and return tasks.

Despite this challenging environment, **Lithuania is overall effectively implementing the Schengen *acquis*, and thereby actively contributing to the well-functioning of the Schengen area**. This evaluation report identifies a number of best practices supporting the effective implementation of the Schengen architecture and describes good operational solutions to address common challenges. However, some measures to swiftly deal with crisis situations, notably at the land border with Belarus, have an important impact on the level of protection of **fundamental rights**, in particular on the *non-refoulement* safeguards.

Lithuania implements efficiently the **European Integrated Border Management**. The State Border Guard Service, the single authority responsible for the overall coordination and implementation of border management based on high quality of risk analysis, continues to be a good practice as it provides a comprehensive situational awareness and effective reaction capabilities. In addition, the necessary structures **are in place to ensure the effective return** of third-country nationals with no legal right to stay, although there is still no mechanism to deal swiftly with subsequent asylum applications lodged for the purpose of delaying return procedures. Lithuania delivers **a reliable contribution to the European Border and Coast Guard** and makes efficient use of European capabilities for border control and return. However, the working procedures and practices used by the standing corps deployed in Lithuania, as well as the equipment used are not sufficiently adapted to the operational conditions and needs in the field.

The quality of the **sea and land border surveillance** carried out by the State Border Guard Service is at a high level and adequate for the circumstances. Lithuania has set up a state-of-the art and comprehensive land border surveillance system at its external land borders. Nevertheless, advance detection equipment and software for drones and other unidentified aerial vehicles is not sufficient at

[1] According to information provided by the Lithuanian authorities.

the land borders thus decreasing the efficiency of measures taken to fight cross-border crime. While the **quality of border checks** is good at the land borders, it needs consistent improvement at the air borders and at the sea borders, where the mobile devices do not allow for the check of chip data. At all borders, **the visa-issuing procedure is deficient.**

Measures in third countries on the application of the **EU common visa policy are well implemented**. The examination of Schengen visa applications is solid, and decisions are generally well-founded. There are, nevertheless, delays in the processing of visa applications and deficiencies were identified in the application of the EU-Armenia visa facilitation agreement.

The **Lithuanian police cooperation system is well established, and Lithuania participates actively to European cooperation.** Nevertheless, a comprehensive human resources strategy for the Lithuanian Police is still missing. The present composition and the structure of the Single Point of Contact are not sufficient to allow it to become a fully integrated hub for exchange of information. Furthermore, Lithuania does not have a formal review mechanism for existing bilateral agreements with the neighbouring Member States, with the aim to increase their operational effectiveness. The procedure to consult the Visa Information System by designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences is not efficiently implemented.

Large-scale IT systems supporting the well-functioning of the Schengen area, notably the Schengen and Visa Information Systems**, are adequately implemented, and Lithuania overall complies with the data protection requirements.** Lithuania has effectively rolled-out the upgraded functionalities of the Schengen Information System, which are well integrated in border, migration and law enforcement processes. However, searches in the Automated Fingerprint Identification System are still not rolled out to end-users in the police and there are some shortcomings in both national applications used by border and law enforcement authorities, which can for instance lead to hits on alerts being missed. The State Data Protection Inspectorate did not yet complete an audit of the data processing operations in both the national Schengen and Visa Information Systems within the required 4-year timeframe. Controllers of these two systems are not carrying out sufficient regular checks and monitoring of access logs. In addition, Lithuania needs to provide for the independent supervision of national security and defence processing activities in these systems.

On the basis of the 2023 Schengen evaluation, the evaluation team has identified five horizontal priorities to strengthen Lithuania's performance in applying the Schengen *acquis*:

1/ Strengthen **border control** providing for sufficient number of trained staff and reaction capabilities;

2/ Guarantee the respect of **fundamental rights**, especially the principle of *non-refoulement*, when applying border-policing measures;

3/ Increase the effectiveness of the **return system** by removing obstacles that hamper the implementation of return procedures;

4/ Enhance the use of **police cooperation** tools, by revising existing police cooperation arrangements with Latvia and Poland to meet current and future operational needs.

5/ Ensure that the State Data Protection Inspectorate **carries out audits of the** data **processing operations in the** National Schengen Information System and the National Visa Information System, at least every four years.

2. RECOMMENDATIONS

The 2023 periodic evaluation of Lithuania resulted in 51 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, 4, 13, 15, 19, 22, 28, 37, 39, 49 and 51, highlighted in bold, should be prioritised.

Lithuania is recommended to:

NATIONAL SCHENGEN FRAMEWORK

Strategic framework

1. develop an international police cooperation strategy complemented by an action plan, taking into consideration the National Serious Organised Crime Threat Assessment and respective capacity building activities;

National capabilities

2. **develop further a comprehensive human resources strategy for the Lithuanian State Border Guard Service and implement such a strategy for the Lithuanian Police to ensure a sufficient number of trained staff adapted to the passenger traffic flow, migratory pressure, and operational challenges**; *[prioritised recommendation]*
3. ensure continuous and specialised training to the Lithuanian Police, with particular focus on international police cooperation tools, anti-corruption, fundamental rights and the Schengen Information System;
4. **ensure continuous and specialised training to the State Border Guard Service at regional and local levels, in particular on document examination, detection of stolen vehicles, fundamental rights and the Schengen and Visa Information System**; *[prioritised recommendation]*
5. improve the coordination between the Data Protection Officer of the data controller and the Data Protection Officers of the end-user authorities in relation to their responsibilities for training for the National Schengen and Visa Information System end-users;

Use of large-scale information systems and respect of data protection requirements

6. roll out the fingerprint functionality in the Schengen Information System (AFIS) to all competent authorities in accordance with Article 33(2) of Regulation (EU) 2018/1861, Article 43(2) of Regulation (EU) 2018/1862 and, as applicable to return alerts, Article 19 of Regulation (EU) 2018/1860;
7. ensure the full display of all available information on hits and alerts for discreet check and misused identity in the VSATIS application and upgrade the query possibilities in both the VSATIS and POLISII application to ensure that end-users can perform all searches as prescribed by Article 9(2) of Regulation (EU) 2018/1861, Article 9(2) of Regulation (EU) 2018/1862 and, as applicable to return alerts, Article 19 of Regulation (EU) 2018/1860;
8. improve the display of alerts, actions to be taken, warning markers, results of searches and misused identity information and enable the multi-category query functionality in the POLISII and VSATIS applications;
9. improve the reporting and exchange of information in the Schengen Information System by:

a) fully implementing the functionality for the statistical reporting on the use of the Schengen Information System and the exchange of supplementary information;

b) ensuring that information related to consultation procedures is exchanged between the SIRENE Bureau and the Migration Department in a format that would allow for automation, including of conversion of the data;

10. improve the alert management in the Schengen Information System by:

a) implementing measures to ensure that refusal of entry and stay and return alerts can be updated on 24-hour basis in accordance with Articles 6(2), 7(2), 8, 9(2), 11(f) and 14 of Regulation (EU) 2018/1860 and Articles 24(3), 26(2), 29(f), 44(2) and (5) of Regulation (EU) 2018/1861;

b) implementing the legal possibility to enter the alerts on vulnerable persons who need to be prevented from travelling;

11. ensure that the emails containing SIRENE forms are deleted from Microsoft Outlook, at the latest one year after the related alert has been deleted from the Schengen Information System.

12. strengthen the security requirements of the National Schengen Information System by

a) strengthening the contingency solutions for the National Schengen Information System, providing for its complete switchover and allowing for a reasonable and reliable geographical redundancy;

b) preventing any unauthorised access to the main data centre and to the SIRENE Office in compliance with Article 10(2) of Regulation (EU) 2018/1861, Article 10(2) of Regulation (EU) 2018/1862 and, as applicable to return alerts, Article 19 of Regulation (EU) 2018/1860;

13. **ensure the independence of the Data Protection Officer of the Information Technology and Communications Department by separating the functions of the Data Protection Officer from the functions of the Head of the Information Security Unit**; *[prioritised recommendation]*

14. improve the data protection requirements for the National Schengen Information Systems by:

a) ensuring that all National Schengen Information System workstations functioning with End-of-life Operating Systems, utilising software for which the support lifecycle has expired, will be decommissioned and replaced by workstations operating with the latest Operating Systems;

b) extending the two-factor authentication mechanism to all workstations and (or) systems having direct access to National Schengen Information System data;

c) ensuring that the SIEM equipment and software is kept updated and that further revised parameters for the automatic log control are set in order to better detect unlawful processing of personal data and thus improve the detection of risks and threats to the National Schengen Information System;

d) ensuring that the Data Protection Officers of the National Schengen Information System end-user authorities are actively involved in the checking of logs;

e) ensuring that all National Schengen Information System end-user authorities are well informed about the procedures for determining personal data breaches and on informing the data controller*;*

Fundamental rights

15. **in accordance with Article 19 of the Charter of Fundamental Rights, Articles 3(b), 4, 7(1) and 13 of the Schengen Borders Code, Article 4(4) of Directive 2008/115/EC, take measures to ensure the full respect of the principle of non-refoulement in cases of rejection of admission, by issuing individualised decisions and ensuring that appeals against non-admission actions are available and accessible in practice; ensure that third country nationals seeking international protection on the territory, including at the border, can effectively access international protection**; *[prioritised recommendation]*

16. establish adequate procedures to detect and refer vulnerable persons;

Data protection supervision

17. ensure that the State Data Protection Inspectorate has the final decision in its staff selection procedures to guarantee its complete independence;

18. ensure that the State Data Protection Inspectorate finds an alternative for an e-signature as a formal (electronic) requirement for launching a complaint/appeal in relation to Schengen Information and Visa Information Systems data processing;

19. **ensure that the State Data Protection Inspectorate finalises the on-going National Schengen Information System audit as soon as possible and carries out at least every four years an audit of data processing operations in the National Schengen Information System, 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 by the national visa/Visa Information System authorities at least every four years in accordance with Article 41 (3) of VIS Regulation and Article 8 (6) of VIS Council Decision**; [*prioritised recommendation*]

20. take the following steps in relation to the supervision of data processing in National Schengen Information and Visa Information Systems:

    a) ensure independent data protection supervision of the processing of personal data in the National Schengen Information System and the Visa Information System carried out by state authorities for purposes of national security or defence;

    b) ensure that the State Data Protection Inspectorate performs frequent inspections of the competent end-user authorities, the External Service Providers as well as of the National Schengen and Visa Information System logs;

Activities of Union bodies

21. 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

22. **conduct a thorough analysis with the other Baltic countries and Poland on the establishment of a common use of these countries' respective liaison officers**; *[prioritised recommendation]*

23. ensure that visa applications are, as a rule, processed within 15 calendar days, also by refraining from carrying out interviews in cases where the consulate has already ascertained the existence of one or more refusal reasons, while still conducting interviews when the examination of the visa application based on the information and the documentation available does not allow a final decision to be taken;

24. instruct the external service provider to only modify application data in the online application portal of Lithuania with the express knowledge and consent of the applicant and guarantee that in these cases the consulate is always made aware of modifications made, and that the original information entered by the applicant can be retrieved easily by the consulate if necessary; and ensure that the external service provider no longer has access to data entered into the portal at the latest seven days after the application has been transferred to the consulate in accordance with Annex X, points B(a), (e) and (h) of the Visa Code;

25. refrain from entrusting the external service provider with the task of affixing printed visa stickers in travel documents, including for long-stay visas;

26. fully implement the EU-Armenia visa facilitation agreement;

27. ensure that all recommendations on data protection aspects concerning the management of the National Schengen Information System are also being followed up for the management of the National Visa Information System;

MANAGEMENT OF THE EXTERNAL BORDERS

Border surveillance

28. **strengthen border surveillance and reaction capacities, including for detection and interception of unauthorised cross border unmanned aerial vehicles flights**; *[prioritised recommendation]*

Border checks

29. bring the performance of first and second line border check procedures in accordance with Article 8 of the Schengen Borders Code by

    a) bringing the queue management system (EVIS) in line with the Schengen Border Code;

    b) enhancing the English language training of border guards;

    c) upgrading the procedures of checking the authenticity of the travel document by ensuring that mobile devices can read the chip of the travel document (Uostas Frontier Station);

30. conduct second line checks at a dedicated location separated from the first line checks and in accordance with the risk indicators and profiles adapted to the composition of the traffic flow (Vilnius and Kaunas Airports);

31. ensure timely checks of the databases during border checks by improving the network connectivity of the VSATIS application;

32. bring the practice of imposing fines to air carriers in compliance with Council Directives 2001/51/EC and 2004/82/EC;

33. bring the procedures of issuing, extension and refusal visas at the border in compliance with Articles 32(2), 35 and 36 and Annex VI to the Visa Code;

34. provide the State Border Guard Service with guidelines for the use of the fingerprint functionality (AFIS) of the Schengen Information System, defining the situations where such queries should be performed;

35. ensure direct access to the Schengen Information System for all custom officers and integrate it better in the customs control process, including though training, to ensure systematic checks of the Schengen Information System in accordance with Article 34(1)(b) of Regulation (EU) 2018/1861 and Article 44(1)(b) of Regulation (EU) 2018/1862;

36. inform data subjects at the external border control about their data processed in the Visa and Schengen Information System, including on how to exercise their data subjects' rights and to whom to send requests, and make this information directly available at the second line check without the data subjects having to request it;

NATIONAL RETURN SYSTEM

37. **increase the effective enforcement of return decisions by establishing a mechanism to deal swiftly with international protection applications lodged for the sole purpose of delaying or hampering a return procedure**; *[prioritised recommendation]*

38. amend the national legislation to ensure an individual assessment of the period for voluntary return, including prolongations beyond 60 days, where necessary;

39. **ensure that entry bans clearly indicate that the third-country national is not allowed to enter and stay in the EU/Schengen area for the full duration of the entry ban**; *[prioritised recommendation]*

40. enhance the effectiveness of the forced-return monitoring system by ensuring an efficient flow of information and by increasing the frequency of monitored in-flight phases;

41. ensure that alternative measures to detention do not amount to de facto detention in accordance with Article 15(1) of Directive 2008/115/EC;

42. amend the legislation to ensure the immediate release of detained third-country nationals, once the reasonable prospect of removal ceases to exist in accordance with Article 15(4) of Directive 2008/115/EC;

MEASURES WITHIN THE AREA OF FREEDOM, SECURITY AND JUSTICE

Exchange of information for cross-border and international police cooperation

43. enhance the use of police cooperation tools by

    a) finalising the full legal and organisational (physical or technical) integration of all national Law Enforcement Authorities into the Single Point of Contact structure;

    b) developing dedicated training and clear written guidelines containing the rules of cross-border law enforcement information exchange, international law enforcement cooperation tools and choice of communication channels to be used in the Single Point of Contact as well as a system to evaluate training effectiveness;

    c) improving information exchange with the police authorities of the other Member States and Europol.

44. ensure full implementation and awareness of the access procedure for law enforcement purposes to the Visa Information System established under Council Decision 2008/633/JHA;

45. urgently improve the national search applications on desktop and mobile devices to carry out single searches for objects and individuals as to have the results from various national and international databases linked into one hit containing all available information with clear instructions on actions to be taken;

46. develop a technical solution 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;

47. step up the use of Europol's Secure Information Exchange Network Application (SIENA) by also extending direct access of national and regional investigative units of competent law enforcement authorities;

48. grant search access to the Europol Information System to investigators from the different law enforcement authorities, along with corresponding training of end-users, and extend the access to the data loader to all competent law enforcement authorities ensuring that all relevant criminal information obtained within ongoing investigations is uploaded when it relates to serious and organised crime and terrorism;

Operational cross-border police cooperation

49. **develop a formal review mechanism for bilateral agreements with the aim to increase their operational effectiveness and revise police cooperation agreements with Poland and Latvia to better meet current operational needs, also engaging regional level to improve the legal framework of cross-border cooperation**; *[prioritised recommendation]*

50. further develop operational cross-border police cooperation by

    a) evaluating the functions and tasks of Lithuanian law enforcement authorities in Border Guard, Customs and Police Cooperation Centre;

    b) improving English and other language skills of police officers responsible for cross-border cooperation matters by providing adequate language courses to ensure sufficient level quality of cross-border cooperation;

    c) raising awareness of all relevant Lithuanian Police structures and competent law enforcement authorities on the possibility and potentiality of cross-border surveillance and on its rules and procedures;

    d) developing a coordinated mechanism for a comprehensive overview on all joint law enforcement patrols to facilitate resource planning and effective cooperation and explore the possibility of having joint patrols and cross border surveillance on coastal waters;

    e) extending the possibility for the hot pursuit for its law enforcement staff beyond those cases when the pursued person is caught in committing an offence;

51. **set up a secure and interoperable communication system between Lithuanian law enforcement agencies and those of Poland to be used during different types of cross-border operations**. *[prioritised recommendation]*